Sumário

Primeiros passos...

Prezado(a) usuário(a)!

Agradecemos que você tenha optado por um produto G Data e esperamos que esteja sempre satisfeito com seu novo software. Caso algo não funcione imediatamente, talvez a nossa documentação da ajuda possa ajudá-lo(a). Para perguntas, críticas e sugestões, a nossa equipe de especialistas no **G Data Suporte técnico** está disponível.

Esta introdução ajuda a instalar seu novo software G Data e fornece algumas dicas práticas para utilização.

Você tem mais alguma dúvida? No software, é possível abrir a qualquer momento a ajuda detalhada do programa. Para isso, basta pressionar no programa a tecla **F1** ou clicar no botão da Ajuda aqui ilustrado.

Suporte técnico

A instalação e utilização do software G Data são intuitivas e descomplicadas. Caso ocorra algum problema, simplesmente entre em contato com os funcionários especializados do nosso Suporte técnico:

www.gdatasoftware.com.br

Instalação

Para o funcionamento correto do software, o seu computador deve atender aos seguintes **requisitos mínimos** dependendo do sistema operacional:

- Microsoft Windows 7 / Vista (32/64bit), memória de trabalho disponível de 1 GB,
- Microsoft Windows XP (SP2 ou superior, 32bit), memória de trabalho disponível de 512 MB.

Se o seu computador for novo de fábrica ou tiver sido protegido até agora por um software antivírus, será possível executar a instalação com as etapas a seguir. Mas, se você tiver a suspeita fundada que o seu computador está infectado com vírus, recomenda-se a realização de um **BootScan** antes da instalação do software G Data. Para isto, leia o capítulo **BootScan**.

Etapa 1

Além da instalação clássica de software com CDs ou DVDs, agora há outras possibilidades da instalação de software:

- **Instalação com CD/DVD**: Para começar a instalação, insira o CD ou DVD do software G Data. Uma janela de instalação é aberta automaticamente.
- **Instalação do pen drive USB**: Caso você tenha comprado o software em um pen drive USB, conecte o pen drive USB com o seu computador. Uma janela de instalação é aberta automaticamente.
- **Download do software**: Para começar com a instalação de uma versão do software baixada da internet, faça simplesmente um clique duplo no arquivo baixado. Uma janela de instalação é aberta automaticamente.

Etapa 2

Agora, clique no botão **Instalar**. Agora, um assistente o ajudará com a instalação do Software no seu computador.

Etapa 3

Durante a instalação, acontece a **ativação do produto**. Aqui você pode ativar o seu software.

- **Inserir o número de registro**: Ao instalar o seu software G Data pela primeira vez, selecione esta opção e, a seguir, insira o número de registro que acompanha o produto. Dependendo do tipo do produto, o número pode ser encontrado, por exemplo, no verso do manual de instruções, no e-mail de confirmação do download do software ou na capa do CD.

  Ao inserir o número de registro, o seu produto será ativado e, além disso, você receberá um e-mail com os dados de acesso para a futura utilização.

  Se tiver problemas na inserção do número de registro, verifique o Número de registro. Dependendo do tipo de letras utilizado, muitas vezes interpreta-se um "I" maiúsculo (como Ida) erroneamente como o número "1" ou a letra "l" (como Ludwig). O mesmo vale para: "B" e "8", "G" e 6, "O" e "0", "Z" e "2".

- **Inserir dados de acesso**: Se você já ativou o seu software G Data anteriormente, então você recebeu seus dados de acesso (**nome de usuário** e **senha**). Para instalar o software G Data novamente ou para registrar mais computadores com uma licença multiusuário, simplesmente insira os seus dados de acesso aqui.

  Você recebe os dados de acesso exclusivamente por e-mail. Os dados de acesso não estão acompanhando o produto.

  Se tiver perdido ou esquecido os seus dados de acesso, clique, para se conectar, no registro **Perdeu os seus dados de acesso?** Uma página será aberta onde será possível inserir novamente o número de registro. Após inseri-los, os dados de acesso serão enviados ao endereço do e-mail informado no registro. Se o seu **endereço de e-mail** mudou nesse período, entre em contato com a nosso **Suporte técnico**.

- **Versão de teste**: Para conhecer o softwareG Data gratuitamente, você pode utilizar simplesmente o nosso acesso de teste temporário. Informe aqui um endereço de e-mail válido e o seu nome e você receberá de nós os dados de acesso via e-mail.

- **Ativar mais tarde**: Se você quiser simplesmente dar uma olhada no software, você pode instalá-lo também sem a informação de dados. Mas, desta forma o programa não descarrega atualizações da internet e, portanto, não haverá uma proteção real contra software malicioso. Você pode informar o número de registro ou os seus dados de acesso a qualquer tempo posteriormente, assim que você executar uma atualização.

O software G Data pode proteger o seu computador eficientemente apenas com atualizações atuais do dia. A utilização do software sem a ativação protege você apenas insuficientemente.

Etapa 4

Talvez você precise reiniciar o seu computador após a instalação. Então, o software G Data estará à sua disposição.

Caso a instalação não inicialize: Pode ser que a **função inicialização automática** de seu computador não esteja configurada corretamente. Então, o software não pode iniciar o procedimento da instalação após a introdução do CD de programa (ou a conexão do pen drive USB na versão do pen drive USB do software G Data) e não é aberta nenhuma janela com qual você possa instalar o software G Data.

- Se, ao invés disso, uma janela de opções for aberta para uma reprodução automática, clique na opção **Executar AUTOSTRT. EXE**.
- e uma janela de seleção não for aberta, procure no seu Windows Explorer a mídia de dados com software G Data e então inicie o arquivo **Setup** ou, conforme o caso, **Setup.exe.**

Assim, aparecerá a janela de instalação de seu software G Data e você pode iniciar a instalação.

Após a instalação

Para abrir a interface de programa do seu software, simplesmente clique duas vezes no **ícone da área de trabalho** ilustrado aqui. Para saber como utilizar a SecurityCenter. leio o capítulo: **SecurityCenter**.

G Data Ícone: Seu software G Data protege seu computador permanentemente contra softwares maliciosos e ataques. Um ícone G Data na barra de tarefas do seu computador alerta você assim que o software determina a necessidade de uma intervenção do usuário. Informações avançadas podem ser obtidas no capítulo: **Para que serve o ícone G Data?**

Verificação rápida: Com a verificação rápida, você pode verificar arquivos de forma simples, mesmo sem precisar iniciar o software. Basta marcar com o mouse os arquivos ou a pasta, por exemplo, no Windows Explorer. Clique então no botão direito do mouse e selecione na janela de diálogo que surge **Verificar a existência de vírus**. Uma verificação automática dos respectivos arquivos será executada.

G Data Triturador: Caso você tenha selecionado o triturador na instalação, este poderá ser acessado por meio do ícone na área de trabalho. Dados jogados no triturador são eliminados de forma que não podem mais ser restaurados, mesmo com ferramentas profissionais de recuperação de dados. Alternativamente, você pode clicar um arquivo com o botão direito do mouse e selecionar **Triturar**. O triturador não está disponível na versão de programa **G DataAntiVirus**.

Após a instalação do softwareG Data **, seu computador inicia diferentemente do habitual**: Se, após a instalação do software G Data, o computador não iniciar diretamente com o Microsoft Windows em uma próxima reinicialização, pode ser em razão de o CD G Data ainda se encontrar dentro da unidade de CD. Ele serve ao mesmo tempo como CD de boot que pode iniciar antes do sistema operacional para executar um BootScan, caso necessário. Simplesmente remova o CD e reinicie o computador da maneira habitual. Informações avançadas podem ser obtidas no capítulo: **BootScan**

SecurityCenter

Após a instalação, a sua proteção antiVirus, em princípio, é executada de forma totalmente automática. A SecurityCenter precisa ser chamada somente quando você desejar acessar uma das muitas funções adicionais do software. Em todos os casos em que o software exija sua intervenção, você será automaticamente lembrado sobre as informações na barra de tarefas do computador.

Com um clique, é possível eliminar do caminho as possíveis ameaças ao seu computador. Para isso, está disponível o símbolo do **Status da proteção**.

Enquanto uma marcação verde estiver acesa ao lado do registro **Segurança** o seu sistema estará protegido.

Um ponto de exclamação vermelho indica que há um perigo iminente para o seu sistema. Você deverá tomar providências imediatas para que seus dados permaneçam protegidos.

Quando você clica no botão **Corrigir**, o software sugere as ações que devem ser executadas para continuar protegendo o seu sistema de forma ideal. Selecione as ações exibidas uma após a outra, até que o status da proteção mostre novamente uma luz verde. O botão muda automaticamente para inativo e só poderá ser utilizado novamente se o status da proteção piorar. Assim o seu software estará novamente no estado mais recente e você poderá fechar novamente a SecurityCenter. Além disso, existem ainda as seguintes mensagens de status:

Um símbolo amarelo indica que é necessária uma intervenção rápida pelo usuário.

Se o símbolo de espaço reservado for exibido, significa que você não ativou a respectiva função de segurança (por ex., proteção contra spam).

Todas as funções e configurações vistas abaixo do símbolo do status da proteção (como **proteção antiVirus** ou **assinaturas de vírus**) podem ser utilizadas quando você desejar se ocupar ativamente da segurança do seu sistema, mas isso não é necessário! Decida você mesmo como deseja se ocupar do assunto da Proteção antivírus. Nas respectivas subseções, você vê detalhadamente as áreas que o seu software ajustou de forma ideal e quais poderão ser melhoradas. Os ícones a seguir indicam o status de segurança da respectiva área.

Configurações: Através desse botão na parte superior direita, você pode acessar todos os diálogos de configuração das diversas áreas do software. Na respectiva área, você também tem a possibilidade de selecionar diretamente o diálogo de configuração adequado.

Para isso, se necessário, leia também o capítulo: **Configurações**

Além disso, à direita, ao lado do símbolo de configuração, podem ser encontradas as seguintes funções adicionais:

Exibir ajuda: No software, é possível abrir a qualquer momento a ajuda detalhada do programa. Para isso, basta pressionar no programa a tecla F1 ou clicar no botão de Ajuda aqui ilustrado.

Registros: O software lista aqui os registros atuais relativos a todas as funções executadas (verificação de vírus, atualização, detecção de vírus etc.).

Criar CD de boot: O BootCD é uma ferramenta útil para tornar computadores já infectados, livres de vírus. Principalmente para computadores que, antes da instalação do software G Data não tinham nenhuma proteção antiVirus, recomenda-se a utilização de um BootCD. As informações sobre como criar e utilizar um **CD de boot** podem ser lidas no capítulo: **BootScan antes da instalação**.

As funções descritas, como por exemplo, a criação de um CD de boot não estão disponibilizadas? Pode ser que a opção **Criar CD de boot** não tenha sido instalada com o software G Data. Esta pode ser facilmente instalada posteriormente, inserindo novamente o CD do software e executando a instalação com a opção BootCD.

Atualizar programa: Quando existirem novas versões do programa do software, você poderá atualizá-las, bem como as informações de vírus, de forma confortável através de cliques. Se obtiver a informação de que uma atualização na Internet está disponível, basta clicar no registro **Atualizar programa**.

Problemas com a atualização na Internet? Informações detalhadas podem ser obtidas no capítulo: **Atualizações**

Informações: Aqui você obtém informações sobre a **versão do programa**. O número da versão pode, por exemplo, ser útil para o contato com o **Suporte técnico**.

Licença

Abaixo do registro **Licença**, no lado esquerdo da interface do programa, você verá por quanto tempo a licença para atualizações de vírus ainda será válida. Em nenhum outro software, as atualizações constantes são tão importantes quanto nos softwares antivírus. Antes que a sua licença expire, o software lembra você automaticamente para renovar a sua licença. A forma mais confortável e descomplicada de fazer isso é pela internet.

O que acontece quando a minha licença expira?

Alguns dias antes de sua licença expirar, aparece uma janela de informações na barra de tarefas. Clicando, abre-se uma caixa de diálogo na qual você pode prorrogar a sua licença sem problemas diretamente, em poucos passos. Clique simplesmente no botão **Comprar agora**, complete os seus dados e a proteção antiVirus está novamente garantida imediatamente. Você receberá a fatura confortavelmente nos próximos dias via correio.

Esta caixa de diálogo aparece apenas após o término do primeiro ano. Depois disso, a sua licença G Data é prorrogada automaticamente a cada ano. Mas você pode cancelar essa assinatura a qualquer hora e sem mencionar as razões.

Como posso receber licenças adicionais/estendidas?

Naturalmente é possível ampliar o número de suas licenças ou fazer uma atualização dos produtos com um maior volume de funções. Se clicar no registro **Estender licenças**, na SecurityCenter, será direcionado para o site de nossa loja online.

Carga na CPU

Sob o título **G Data**, você vê a carga atual ocupada pelo software em seu computador. Abaixo, sob a legenda **Sistema** - você vê a utilização total atual do seu computador. Durante as verificações, a utilização do sistema pelo software G Datapode ser altíssima, mas, durante a operação normal da sentinela, o software G Data utiliza muito pouco a capacidade do processador. Portanto, se o seu computador reagir de forma mais lenta do que a habitual, aqui você poderá detectar rapidamente se o software G Data está momentaneamente executando uma verificação intensiva ou se o computador está sendo restringido por um outro motivo que não esteja relacionado à verificação do sistema.

Além disso, o software G Data está instalado de forma que o seu computador só faz a verificação se não estiver sendo utilizado. Como um protetor de tela, a verificação de vírus ocorre sempre só quando você não é perturbado. Naturalmente a proteção antiVirus permanente através da sentinela de vírus está completamente ativa o tempo todo.

- **Verificação de vírus**: A verificação regular, se não há vírus ou programas maliciosos aninhados no seu computador.
- **Sentinela de vírus**: A proteção geral do seu computador contra software malicioso invasor.

Proteção AntiVirus

Nesta área, você recebe informações sobre quando foi a última vez que o seu computador foi verificado por vírus e se a sentinela de vírus o protege ativamente contra infecções no momento.

Última verificação de vírus

Aqui é exibido quando o computador foi totalmente controlado pela última vez, quanto à infecção por vírus. Quando esse registro estiver marcado em vermelho, você deverá executar o mais rápido possível uma verificação de vírus. Para isto, basta clicar no registro e poderá iniciar o processo de verificação, clicando no botão **Verificar computador**. Após a verificação, o registro estará marcado em verde, uma indicação que uma verificação de vírus foi feita em um período suficiente.

Para saber como é o processo de uma verificação de vírus e o que deverá ser feito se realmente um vírus for encontrado, leia o capítulo: **O que ocorre em uma verificação de vírus?**

Sentinela de vírus

A Sentinela de vírus deve sempre estar ativa. Se desejar desativar a sentinela em algum momento ou desejar efetuar alterações nas configurações, clique no registro **Desativar sentinela de vírus**.

Verificação de vírus e sentinela de vírus: Ambas as funções servem para proteger o seu computador contra infecções, mas têm uma abordagem diferente.

- A **Sentinela de vírus** verifica continuamente o seu computador quanto à existência de vírus e controla os processos de gravação e leitura; assim que um programa desejar executar funções maliciosas ou propagar arquivos danosos, a sentinela de vírus o impede. A Sentinela de vírus é uma proteção importante! Ela não deve nunca ser desativada.

- A **Verificação de vírus** é uma proteção adicional. Ela verifica se um vírus não se encontra no seu sistema. Uma verificação de vírus encontraria mesmo os vírus que foram copiados para o seu computador antes da instalação do software G Data ou que você tenha recebido com a Sentinela de vírus desativada. Uma verificação de vírus deve ser feita em intervalos regulares, preferencialmente em períodos automáticos, durante os quais o seu computador não for necessário.

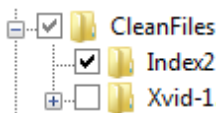
Menu de seleção

Clicando diretamente no título **Proteção antiVirus**, aparecerá uma seleção de ações que podem ser efetuadas diretamente aqui.

Verificar computador: Quando desejar controlar o seu computador de forma independente da verificação automática (p. ex., devido a uma suspeita de vírus), bastará clicar neste registro. O seu computador será diretamente verificado quanto a infecções por vírus. Para isso, leia também o capítulo **O que ocorre em uma verificação de vírus**.

Verificar memória e inicialização automática: Através desta opção, para todos os Processos em andamento são verificados os arquivos de programa e as bibliotecas de programas (DLLs). Dessa forma, os programas maliciosos poderão ser removidos diretamente da **Memória** e da **Área de inicialização automática**. Vírus ativos podem ser removidos diretamente, sem que o disco rígido tenha que ser totalmente pesquisado. Como essa verificação pode ser executada relativamente rápida, é recomendável fazê-la constantemente no escopo de uma verificação de vírus automática. Essa função não é uma substituição de um controle de vírus constante dos dados armazenados, ela é apenas uma complementação.

Verificar diretórios/arquivos: Através dessa opção, você verifica a existência de vírus em unidades, diretórios ou arquivos. Ao clicar nesta ação, uma opção de diretório e arquivo é aberta. Aqui é possível verificar objetivamente a existência de infecção de vírus em arquivos individuais e também em diretórios completos.

Na árvore de diretórios (à esquerda), clicando nos sinais (+), é possível abrir e selecionar os diretórios cujo conteúdo será então exibido na visualização de arquivo. Cada diretório ou arquivo com uma marcação será verificado pelo software. Se nem todos os arquivos tiverem que ser verificados em um diretório, haverá uma marcação em cinza nesse diretório.

Verificar mídias removíveis: Com esta função, verifique **CD-ROMs** ou **DVD-ROMs**, **cartões de memória** ou **pen drives** quanto à infecção por vírus. Ao clicar nessa ação, todas as Mídias removíveis que estiverem conectadas ao seu computador (ou seja, também CDs inseridos, cartões de memória ou Discos rígidos conectados por USB ou Pen drives) serão verificadas. Observe que o software não poderá naturalmente remover vírus de mídias que não permitam acesso à gravação (p.ex., CD-ROMs gravados). Uma eventual detecção de vírus será registrada.

Verificar a existência de Rootkits: Os **Rootkits** tentam escapar dos métodos comuns de detecção de vírus. Com essa função, é possível procurar por rootkits de forma objetiva, sem ter de executar uma verificação completa dos discos rígidos e dados armazenados.

Desativar verificação em modo ocioso: Enquanto a sentinela de vírus protege o seu sistema permanentemente contra software malicioso, a **verificação em modo ocioso** é uma verificação inteligente de vírus que verifica todos os arquivos do seu computador continuamente por infecções de vírus. A verificação em modo ocioso trabalha como uma proteção de tela, apenas quando você não necessita do seu computador por um tempo. Assim que você continuar a trabalhar, ela para e garante o desempenho ideal para o trabalho.

Naturalmente, o seu computador continua protegido pela sentinela de vírus, mesmo se a verificação em modo ocioso for desativada. Isso pode ser útil se você, por exemplo, preferir iniciar uma verificação de vírus do sistema manualmente.

Desativar sentinela de vírus: Com esta opção, é possível desativar a **Sentinela de vírus**, em caso de necessidade, e também ativá-la novamente. Isso pode ser útil, p.ex, quando uma grande quantidade de dados em seu disco rígido é copiada de um local para outro ou para rodar processos de exibição que ocupam muito espaço na memória (copiar DVDs e outros). Você deverá desativar a sentinela de vírus apenas pelo período necessário. Deve-se ter a certeza de que o sistema durante esse período, se possível, não esteja conectado à Internet ou possa acessar dados novos e não verificados (p.ex, através de CDs, DVDs, placas de memória ou dispositivos USB).

Quarentena: A quarentena é uma área protegida dentro dentro do software onde os arquivos infectados são armazenados de forma codificada e, dessa forma, o vírus não pode mais ser repassado a outros arquivos. Leia para isso também o capítulo: **Como funciona a quarentena?**

Configurações:Com este botão, você pode acessar opções de configuração básicas, se for necessário. Para isso, leia o capítulo: **Configurações - AntiVirus**

Assinaturas de virus

Nesta área, você recebe informações sobre as últimas atualizações do programa.

Última atualização

Aqui se visualiza quando foi a última vez que o seu computador recebeu as atuais assinaturas de vírus da internet. Quando esse registro estiver marcado em vermelho, você deverá executar o mais rápido possível uma atualização de vírus. Clique simplesmente no registro e selecione a opção **Atualizar assinaturas de vírus**.

Próxima atualização

Nesse registro é possível visualizar a próxima atualização prevista.

Assinaturas de vírus: Vírus e outros programas maliciosos podem ser reconhecidos por atributos característicos. Seu software G Data possui funções que detectam os vírus também pelo seu comportamento. A detecção e o combate ao respectivo programa malicioso ficam incomparavelmente mais rápidos e mais eficientes com uma assinatura de vírus, comparável com um mandado de captura. A proteção antiVirus ficará realmente segura apenas com a atualização regular desses mandados de captura dos bancos de dados G Data na internet.

Menu de seleção

Clicando diretamente no título **Assinaturas de vírus**, aparece uma seleção de ações que podem ser efetuadas diretamente aqui.

Atualizar assinaturas de vírus: Normalmente, as atualizações das assinaturas de vírus são efetuadas de forma automática. Caso queira efetuar uma atualização imediatamente, clique neste botão.

Desativar atualizações automáticas: Caso que você não queira que o software G Data cuide da atualização das assinaturas de vírus automaticamente, você pode selecionar esta opção. No entanto, a desativação significa um alto risco de segurança e deve ser efetuada apenas em casos excepcionais.

Configurações: Com este botão, você pode acessar opções de configuração básicas, se for necessário. Para isso, leia o capítulo: **Configurações - AntiVirus**

Proteção da web

Nesta área você pode ativar ou desativar a proteção da web. A proteção da web é um módulo que reconhece e, eventualmente, elimina automaticamente ameaças durante a navegação na internet ou durante downloads. Ela serve como apoio adequado da sentinela de vírus e bloqueia websites maliciosos e downloads já antes de serem acessados.

Se uma página da internet for reconhecida como ameaça pelo software G Data, você receberá, em vez da website, uma página de informações da G Data no navegador.

Menu de seleção

Clicando diretamente no título **Proteção da web**, aparecerá uma seleção de ações que podem ser efetuadas diretamente aqui.

Definir exceções: A proteção da web cuida para que você não seja vítima de sites infectados ou fraudulentos. Em alguns raros casos, pode ocorrer que uma página da Internet não seja corretamente exibida, apesar de originar de um ofertante seguro. Nesses casos, você pode colocar os endereços da Internet na Whitelist, ou seja você pode defini-la, como exceção e a proteção da web não a bloqueará mais. Leia no capítulo **Definir exceções** como isso é feito.

Whitelist: Uma seleção de objetos (p.ex. páginas da internet) que são considerados inofensivos pelo usuário e que não são verificados especialmente.

Desativar Proteção da web: A desativação da Proteção da web pode proporcionar, p.ex., uma vantagem de tempo em grandes downloads de fonte segura. A princípio, o seu computador é protegido pela sentinela de vírus, mesmo sem proteção da web. Entretanto, você deverá abrir mão da proteção da web apenas em casos excepcionais.

Configurações: Com este botão, você pode acessar opções de configuração básicas, se for necessário. Para isso, leia o capítulo: **Configurações - Proteção da web**

Firewall

Um firewall protege o seu computador de ser "espionado". Ele verifica que dados e programas da Internet ou rede, chegam em seu computador e que dados são enviados pelo seu computador. Assim que algo indicar que os dados em seu computador foram reproduzidos ou descarregados indevidamente, o firewall dá um alarme e bloqueia a troca de dados indevida.

Menu de seleção

Clicando diretamente no título **Firewall**, aparece uma seleção de ações que podem ser efetuadas diretamente aqui.

Abrir firewall: Com esta função, você abre o firewall G Data numa outra janela e pode configurá-lo extensamente. Mas, normalmente isso não será necessário. Todas as configurações básicas podem ser controladas pela interface de programa SecurityCenter.

Desativar piloto automático: Geralmente é razoável utilizar o firewall na função **Piloto automático**. Ele rodará praticamente em segundo plano e o protegerá, sem a necessidade de grandes configurações.

Utilizando o firewall sem o piloto automático, aparece, em casos de dúvidas, uma janela de diálogo, na qual você pode otimizar as características do sistema passo a passo. Esse é um dispositivo útil para usuários experientes. Mas normalmente não é necessário desativar o piloto automático.

Desativar firewall: O firewall pode ser desativado se for necessário. O seu computador continua conectado com a internet e outras redes, mas **não** é mais protegido pelo firewall contra ataques de espionagem.

Configurações: Com este botão, você pode acessar opções de configuração básicas, se for necessário. Para isso, leia o capítulo: **Configurações - Firewall**

Backup

Com a progressiva digitalização da vida diária, a utilização de serviços de música on-line, câmeras digitais e correspondências de e-mail, é cada vez mais importante proteger os seus dados pessoais. Seja por causa de erros de hardware, um engano ou um dano causado por vírus ou ataques de hacker: os seus documentos particulares devem ser protegidos regularmente. O software G Data assume essa tarefa para você, protegendo assim a sua documentação e arquivos importantes, sem que você tenha que pensar constantemente no assunto.

Menu de seleção

Quando você clica no título **Backup**, é possível abrir a interface do programa da área de backup.

Abrir backup: Com essa função, é possível abrir a área de backup e realizar todas as configurações necessárias. Na SecurityCenter é sempre indicado quando ocorreu o último backup.

Proteção contra spam

Ofertas, anúncios, boletins informativos – a onda de e-mails indesejados aumenta cada vez mais. A sua caixa de entrada está inundada graças a uma grande quantidade de e-mails indesejados? O software G Data protege com segurança contra lixos de spam, bloqueia de forma eficiente remetentes de spam e evita reconhecimentos errôneos devido à combinação de critérios modernos de verificação de spam.

Menu de seleção

Quando você clica no título **Proteção contra spam**, aparece uma opção de ações que você pode executar diretamente.

Protocolo: Spam: Aqui você obtém uma visão geral detalhada sobre todos os e-mails que foram classificados como spam pelo software G Data. Através do botão **Atualizar**, você pode solicitar o status dos dados do software; através do botão **Excluir**, você remove todos os registros selecionados até o momento. Naturalmente, os próprios e-mails em seu programa de e-mail não serão excluídos nesse processo.

Através do botão **Na Whitelist**, você pode colocar diversos e-mails marcados na **Whitelist** para que os respectivos endereços de e-mail sejam em geral excluídos de outra verificação de spam. Através do botão **Na Blacklist**, você pode colocar um e-mail marcado na **Blacklist** e, com isso, verificar os respectivos endereços de e-mail especialmente quanto a elementos de spam.

Protocolo: Nenhum spam: Aqui você obtém uma visão geral detalhada sobre todos os e-mails que não foram definidos como spam pelo softwareG Data. Através do botão **Atualizar** , você pode solicitar o status dos dados do software; através do botão **Excluir**, você remove todos os registros selecionados até o momento. Naturalmente, os próprios e-mails em seu programa de e-mail não serão excluídos nesse processo.

Whitelist: Através da Whitelist você pode excluir determinados endereços de remetentes ou domínios, explicitamente da suspeita de spam. Para isso, basta inserir no campo **Endereços/Domínios** o endereço de e-mail desejado (por ex., newsletter@informationsseite.de) ou o domínio (por ex., informationsseite.de) que deseja excluir da suspeita de spam e o softwareG Data não tratará e-mails desse remetente ou do domínio remetente como spam. Através do botão **Importar**, você também pode adicionar listas prontas de endereços de e-mails ou domínios na Whitelist. Os endereços e domínios deverão estar um abaixo do outro em linhas individuais na lista. Como formato, é utilizado um arquivo simples em txt que pode ser criado também com o Windows Notepad. Através do botão **Exportar**, você também pode exportar uma Whitelist como arquivo de texto.

Blacklist: Através da Blacklist, você pode colocar determinados endereços de remetentes ou domínios explicitamente em suspeita de spam. Para isso, basta inserir no campo **Endereços/Domínios** o endereço de e-mail desejado (por ex., newsletter@megaspam.de.vu) ou o domínio (p.ex., megaspam.de.vu) que deseja colocar em suspeita de spam e o software G Data tratará e-mails desse remetente ou do domínio remetente em geral como e-mails com altíssima probabilidade de spam. Através do botão **Importar**, você também pode adicionar listas prontas de endereços de e-mails ou domínios na Blacklist. Os endereços e domínios deverão estar um abaixo do outro em linhas individuais na lista. Como formato, é utilizado um arquivo simples em txt que pode ser criado também com o Windows Notepad. Através do botão **Exportar**, você também pode exportar uma Blacklist como arquivo de texto.

Desativar proteção contra spam: Aqui é possível, em caso de necessidade, desativar a proteção contra spam no seu computador, por exemplo, se você não tiver nenhum programa de e-mail instalado no seu computador.

Configurações: Com este botão, você pode acessar opções de configuração básicas, se for necessário. Para isso, leia o capítulo: **Configurações - AntiSpam**

Proteção infantil

Com a proteção infantil é possível controlar o comportamento na navegação e a utilização do computador para suas crianças.

A Proteção infantil não é instalada com a instalação padrão do software G Data. Mas ela pode ser instalada posteriormente a qualquer momento.

Menu de seleção

Clicando no título **Proteção infantil**, aparece uma seleção de ações que podem ser efetuadas diretamente aqui.

Abrir Proteção infantil: Com esta função, você abre a Proteção infantil G Data em uma outra janela e você pode configurá-la amplamente.

Ativar para: Como administrador, você pode ativar ou desativar a Proteção infantil para todos os outros usuários do seu computador. A edição das configurações de segurança ocorre na própria interface do programa da proteção infantil.

Para utilizar a Proteção infantil, é preciso colocar a marcação em **Processar conteúdo da internet (HTTP) na área da proteção da web do software** G Data , caso contrário a proteção infantil não funciona corretamente. Você encontra essas opções em **Configurações > Proteção da web > Conteúdo da internet (HTTP)**.

Otimizador

Desde o lembrete automático para as Windows Updates, desfragmentação automática periódica, até a remoção regular de registros desnecessários do Registro e arquivos temporários, com o Otimizador, você tem uma ferramenta nas mãos que torna o seu sistema Windows significativamente mais rápido e claro.

Será exibido quando o último procedimento de otimização foi executado.

Menu de seleção

Clicando diretamente no título **Otimizador**, aparecerá uma seleção de ações que podem ser efetuadas diretamente aqui.

Executar agora a otimização: Assim, você inicializa a otimização independentemente de planos de tempo existentes.

Restaurar: Em cada alteração executada, o software define um ponto de restauração. Se uma das otimizações executadas tiver causado resultados indesejados, ela poderá ser desfeita e o estado do sistema antes da respectiva alteração poderá ser restaurado. Para isso, selecione com o mouse a área até onde você deseja executar a restauração e clique no botão **Restaurar**.

Programação: Você também pode automatizar a otimização do seu computador. Para saber como funciona, leia o capítulo: **Programação**

Configurações: Com este botão, você pode acessar opções de configuração básicas, se for necessário. Para isso, leia o capítulo: **Configurações - Otimizador**

Cofre de dados

O **Cofre de dados** serve como um cofre de banco para a proteção de dados sensíveis. Um cofre pode ser usado, por ex., como uma unidade adicional como uma partição adicional do disco rígido e pode ser operado facilmente. Para criar e gerenciar cofres, na **SecurityCenter**, acesse o cartão de registro **Mais funções** e ali o registro **Sem cofre** à direita, próximo do registro **Cofre de dados**. Aparecerá a opção **Criar novo cofre**. Clique nessa opção e siga os passos seguintes, determinados pelo assistente.

Para processar cofres existentes, clique no botão **Configurar**. Na janela de diálogo para o gerenciamento do cofre, você pode criar novos cofres mas também excluir cofres existentes ou abrir ou fechar.

> Você pode abrir ou fechar cofres existentes confortavelmente pelo ícone G Data. Clique com o botão direito do mouse no ícone G Data na área de trabalho e selecione os cofres desejados em **Abrir cofre** / **Fechar cofre**.

Assistente para a criação de um cofre de dados

O assistente ajuda para a criação de um cofre de dados. Clique em no botão **Continuar** para avançar.

Localização e tamanho do cofre

Agora, informe onde o cofre deve ser gravado e qual será o tamanho do cofre. Para isso, você tem duas possibilidades essencialmente diferentes:

- **Diretório protegido** (**Criar cofre em um diretório protegido**): Aqui o cofre é visualizado praticamente como uma partição adicional do disco rígido, pode ser selecionado como um disco rígido e comporta-se em todas as circunstâncias como um disco rígido. Aqui, você seleciona em que mídia (por ex. **Mídia de dados local (C:)**) o cofre deve ser criado. Cofres criados em um diretório protegido podem ser visualizados no seu computador apenas se o software G Data estiver instalado no seu computador. Se desinstalar o software, os cofres de dados criados não podem ser mais visualizados.

- **Qualquer local de gravação** (**Criar cofre em um diretório protegido**): O cofre é gerenciado praticamente como uma pasta no seu disco rígido. E, como uma pasta, ele pode ser movido, copiado e também apagado. Cofres criados em qualquer local de gravação são visíveis no computador como arquivos com a extensão de arquivo **ts4**.

Em seguida, selecione um **tamanho de cofre** através do posicionamento adequado do botão deslizante. Você terá tanto espaço quanto existir ainda no local de gravação selecionado. Mas, geralmente você deverá permanecer abaixo de 2 GB para quer o seu sistema de computador não esteja comprometido por razões de falta de memória.

O botão à direita do botão deslizante oferece uma possibilidade rápida para a seleção do tamanho do cofre. Você pode definir o tamanho do cofre exatamente, por exemplo, ou definir o tamanho adequado para gravá-lo possivelmente em um CD, DVD ou BluRay.

Clique agora no botão **Continuar**.

Parâmetros do cofre

Nesta janela de diálogo você pode efetuar as seguintes informações e configurações para o cofre:

- **Nome do cofre**: O nome com qual o cofre será gerenciado pelo software G Data.
- **Descrição**: Uma breve descrição adicional que contém, por ex., informações sobre o conteúdo do cofre.
- **Sistema de arquivos**: Aqui você pode determinar se a unidade virtual que gerou o cofre utiliza o sistema de arquivos FAT ou NTFS. Geralmente o registro Seleção Automática deve permanecer aqui.
- **Selecionar a unidade do cofre automaticamente**: O cofre aparece no seu computador como uma unidade de disco rígido. Aqui você pode atribuir uma letra de unidade fixa para o cofre ou deixar o sistema escolher automaticamente. Geralmente recomenda-se a seleção automática.
- **Atribuir unidade**: Esta seleção é disponível apenas se o software não selecionar a unidade do cofre automaticamente.

Clique agora no botão **Continuar**.

Acesso ao cofre

Aqui você pode informar uma senha para um cofre. Para isso, clique no botão **Adicionar**. Agora, no campo de diálogo que aparece, informe a senha desejada em **Senha** e **Repetir senha**. A senha será aceita apenas se as duas entradas de senhas forem idênticas. Isso deve proteger você contra a atribuição de uma senha que, por um erro de digitação, não poderá ser restaurada por você mesmo.

Clique em **Adicionar** para ativar a senha e, em seguida, em **Continuar** para finalizar a configuração do cofre.

Na criação de um cofre, você pode atribuir várias diferentes senhas e definir diferentes permissões. Assim, você pode criar um cofre para você mesmo, no qual você pode ler e modificar arquivos, e, com uma senha, permitir o acesso de outras pessoas para que estas possam ler o conteúdo, mas não modificar.

Se selecionar o cofre após a sua criação e clicar no botão **Permissão**, você terá as seguintes possibilidades de configuração:

Editar inicialização automática: Em cada cofre encontra-se um diretório com o nome **Inicialização automática**. Quando esta opção estiver definida para **Sim**, os arquivos executáveis existentes serão iniciados automaticamente com a abertura do cofre.

Abrir no modo 'Somente leitura': Um usuário que fizer o login com o método de acesso somente leitura não poderá salvar ou alterar os arquivos existentes no cofre. Ele só poderá lê-los.

Abrir como mídia removível: O software G Data abre os cofres de dados no Explorer como discos rígidos locais. Quando desejar que o cofre seja visível no sistema como Mídia de dados removível marque esta opção.

Uso compartilhado: A marcação nesta opção possibilita o uso compartilhado do diretório do cofre para outros computadores na rede. **Advertência**: Nesta configuração, o acesso ao cofre é possível sem a necessidade de digitação de senha. Neste ponto, recomendamos um uso cuidadoso e uma escolha consciente do uso compartilhado do cofre. O uso compartilhado do cofre para todos os usuários da rede, não faz sentido, porque de qualquer forma os dados estarão acessíveis a todos.

Fechar o cofre após o logoff do usuário: Esta opção, deve permanecer ativada por via de regra, porque quando o cofre permanece aberto após o logoff do usuário, outros poderão ver seu conteúdo.

Configuração do cofre

O Assistente de criação do cofre informa, na última etapa, sobre os parâmetros de configuração. Quando desejar alterar essas configurações, clique no botão **Voltar**. Quando estiver satisfeito com as configurações, clique em **Criar**. O cofre de dados virtual e codificado será criado no disco rígido do seu computador. Com o último clique no botão **Finalizar**, o cofre será criado e aberto diretamente, se desejar.

Configurações

Na área **Configurações**, você pode configurar os respectivos módulos dos programas de acordo com as suas preferências. Via de regra, não é necessário executar aqui as alterações, pois o software G Data já foi configurado de maneira ideal para o seu sistema na instalação.

AntiVirus

Aqui você encontra todas as possibilidades de configuração sobre o tema proteção antiVirus.

Sentinela

Na caixa de diálogo **Opções** da **Sentinela de vírus**, você tem as seguintes opções de configuração. Somente em casos especiais, é necessário fazer alterações aqui:

- **Status da sentinela**: Aqui você determina se a sentinela deve ser ativada ou desativada.
- **Utilizar mecanismos**: O software trabalha com dois **mecanismos** (engine = máquina/motor em inglês), ou seja, dois programas de verificação de vírus independentes entre si. Cada mecanismo, por si só, já protegeria contra vírus, em alta escala, mas, exatamente a combinação de ambos os mecanismos, oferece os melhores resultados. Em computadores antigos e lentos, é possível, mediante a utilização de apenas um único mecanismo, acelerar a verificação de vírus; no entanto, via de regra, deve-se manter a configuração **Ambos os mecanismos**.
- **Arquivos infectados**: Ao detectar um vírus, a configuração padrão pergunta o que você deseja fazer com o vírus e o arquivo infectado. Quando desejar executar sempre a mesma ação, poderá definir isto aqui. A máxima segurança para os seus dados é oferecida pela configuração **Desinfectar (se não for possível: para quarentena) quarentena))**.
- **Pastas infectadas**: Defina aqui se as **pastas** (por exemplo, arquivos com a extensão **RAR**, **ZIP** ou também **PST**) deverão ser tratados de forma diferente dos arquivos normais. No entanto, observe que mover um arquivo compactado para a quarentena pode danificá-lo, de forma que ele também não poderá mais ser usado após movê-lo de volta. Por essa razão, em caso de pastas infectadas, recomenda-se decidir caso a caso e selecionar **Perguntar as ações desejadas**.

- **Proteção do sistema**: Se o monitoramento do comportamento for ativado, toda a atividade no sistema será monitorada independentemente da sentinela de vírus. Assim, identificam-se também pragas que ainda não possuem uma assinatura. O monitoramento do comportamento protege especialmente contra modificações na inicialização automática e no arquivo host.

Exceções

Clicando no botão **Exceções** você pode excluir determinadas unidades, diretórios ou arquivos da verificação e, dessa forma, acelerar significativamente o reconhecimento de vírus. Para isso, proceda da seguinte forma:

1. Clique no botão **Exceções**.

2. Na janela **Exceções da sentinela**, clique em **Nova**.

3. Selecione agora se deseja que a exceção seja aplicada a uma unidade de disco, um diretório, arquivo ou tipo de arquivo.

4. Então, selecione abaixo o diretório ou a unidade que deseja proteger. Para proteger arquivos, digite o nome completo do arquivo no campo de entrada na máscara de arquivos. Aqui também é possível trabalhar com **Espaços reservados**.

   A forma de funcionamento dos Espaços reservados é a seguinte:

   - O **ponto de interrogação** (?) é substituto para caracteres individuais.
   - * O **asterisco** (*) é substituto para seqüências de caracteres inteiras.

   Para, por exemplo, proteger todos os arquivos com a extensão **.sav** , digite ***.sav**. Para proteger uma seleção especial com nomes de arquivo sequenciais, (p.ex., text1.doc, text2,doc, text3.doc), digite, por exemplo, **text?.doc**.

Esse processo pode ser repetido quantas vezes desejar e também, é possível excluir ou modificar novamente as exceções existentes.

Avançado

Defina com um clique no botão **Avançado** que verificações adicionais deverão ser executadas pela Sentinela de vírus. Normalmente, nenhuma outra configuração é necessária aqui.

- **Modo**: Aqui você pode determinar se os arquivos na execução devem ser verificados apenas na leitura ou na escrita e na leitura. Se a verificação acontecer na escrita de um arquivo, verifica-se diretamente na criação de um novo arquivo ou uma versão do arquivo se este arquivo eventualmente foi infectado por um processo desconhecido. Caso contrário, os arquivos serão verificados apenas quando lidos por programas.
- **Verificar acessos à rede**: Se houver uma conexão de rede do seu computador para computadores desprotegidos (p.ex., Notebooks de terceiros), é recomendável verificar também a existência da transferência de programas maliciosos no acesso à rede. Se utilizar o seu computador de forma individual sem acesso à rede, essa opção não precisa ser ativada. Se tiver instalado uma proteção antivírus em todos os computadores da rede, recomenda-se também, desativar essa opção, porque alguns dados poderão ser verificados duplamente, o que causará um efeito negativo na velocidade.
- **Heurística**: Na análise heurística, os vírus não são reconhecidos apenas por meio da atualização de vírus, obtida regularmente online, mas, com base em determinadas características típicas de vírus. Esse método é mais uma vantagem de segurança, no entanto, em raros casos, pode levar a um alarme falso.
- **Verificar pastas (compactadas)**: A verificação de dados em arquivos compactados (reconhecidos através das extensões de arquivo **ZIP**, **RAR** ou também **PST**) demanda muito tempo e normalmente pode ser ignorada quando a Sentinela de vírus estiver, em geral, ativada no sistema. Para aumentar a velocidade da verificação de vírus, você pode limitar o tamanho das pastas, que serão verificadas, para um determinado valor em megabytes.
- **Verificar pastas de e-mail**: Como o software já verifica a infecção de vírus na entrada e na saída de e-mails, na maioria dos casos, é recomendável não fazer a verificação regular da pasta de e-mail, porque esse procedimento, dependendo do tamanho da pasta, poderá demorar alguns minutos.

- **Verificar áreas do sistema na inicialização do sistema**: As áreas de sistema (p.ex., setores de boot) do seu computador não devem ser ignoradas no controle de vírus. Aqui você pode definir se essas áreas devem ser verificadas na **inicialização do sistema** ou na **troca de mídia (por ex., novo** CD-ROM). Normalmente, pelo menos uma dessas duas funções deve estar ativada.
- **Verificar áreas de sistema na troca de mídia**: As áreas de sistema (p. ex., setores de boot) do seu computador não devem ser ignoradas no controle de vírus. Aqui você pode definir se essas áreas devem ser verificadas na inicialização do sistema ou na **troca de mídia** (p.ex., novo CD-ROM). Normalmente, pelo menos uma dessas duas funções deve estar ativada.
- **Verificar Discador/Spyware/Adware/Riskware**: Com este software, o seu sistema pode ser verificado também quanto a **Discadores** e outros programas maliciosos (**spyware**, **adware** e **riskware**). Aqui, trata-se de programas que estabelecem caras e indesejadas conexões à Internet e não ficam nada atrás dos vírus em relação ao seu potencial de dano comercial, que p.ex., armazenam secretamente o seu comportamento na navegação ou até mesmo todos os dados digitados (e com isso também suas senhas) e, na próxima oportunidade, encaminham através da Internet a terceiros.
- **Verificar somente arquivos novos ou alterados**: Se você ativar esta função, serão verificados somente os arquivos que não são alterados há muito tempo e que antes tinham sido reconhecidos como inofensivos. Isso leva a um ganho de desempenho no trabalho diário – sem risco de segurança.

Verificação manual de vírus

Aqui é possível efetuar configurações básicas do programa para a **Verificação de vírus**. No entanto, isso não é necessário para o funcionamento normal.

- **Utilizar mecanismos**: O software trabalha com dois **mecanismos** (engine = máquina/motor em inglês), ou seja, dois programas de verificação de vírus independentes entre si. Cada mecanismo, por si só, já protegeria contra vírus, em alta escala, mas, exatamente a combinação de ambos os mecanismos, oferece os melhores resultados. Em computadores antigos e lentos, é possível, mediante a utilização de apenas um único mecanismo, acelerar a verificação de vírus; no entanto, via de regra, deve-se manter a configuração **Ambos os mecanismos**.
- **Arquivos infectados**: O software encontrou um vírus? Na configuração padrão, o software pergunta o que você deseja fazer com o vírus e o arquivo infectado. Quando desejar executar sempre a mesma ação, poderá definir isto aqui. A máxima segurança para os seus dados é oferecida pela configuração **Desinfectar (se não for possível: para quarentena) quarentena))**.
- **Pastas infectadas**: Defina aqui se as **pastas** (por exemplo, arquivos com a extensão **RAR**, **ZIP** ou também **PST**) deverão ser tratadas de forma diferente dos arquivos normais. No entanto, observe que mover um arquivo compactado para a quarentena pode danificá-lo, de forma que ele também não poderá mais ser usado após movê-lo de volta. Por essa razão, em caso de pastas infectadas, recomenda-se decidir caso a caso e selecionar **Perguntar as ações desejadas**.
- **Em caso de sobrecarga suspender a verificação de vírus**: Normalmente, uma verificação de vírus só pode ocorrer quando seu computador não estiver sendo utilizado. Se você precisar utilizar o computador, a verificação de vírus é pausada para que o computador esteja disponível na velocidade comum. A verificação de vírus também é executada durante as suas pausas no trabalho.

Exceções

Clicando no botão **Exceções**, você pode excluir determinadas unidades, diretórios e arquivos da verificação e, dessa forma, acelerar significativamente o reconhecimento de vírus. Para isso, proceda da seguinte forma:

1. Clique no botão **Exceções**.

2. Clique, na janela **Exceções para a verificação manual do computador**, em **Novo**.

3. Selecione agora se deseja que a exceção seja aplicada a uma unidade de disco, um diretório, arquivo ou tipo de arquivo.

4. Então, selecione abaixo o diretório ou a unidade que deseja proteger. Para proteger arquivos, digite o nome completo do arquivo no campo de entrada na máscara de arquivos. Aqui também é possível trabalhar com **Espaços reservados**.

   A forma de funcionamento dos Espaços reservados é a seguinte:

   - O **ponto de interrogação** (?) é substituto para caracteres individuais.
   - * O **asterisco** (*) é substituto para seqüências de caracteres inteiras.

   Para, por exemplo, proteger todos os arquivos com a extensão **.sav** , digite ***.sav**. Para proteger uma seleção especial com nomes de arquivo sequenciais, (p.ex., text1.doc, text2,doc, text3.doc), digite, por exemplo, **text?.doc**.

Esse processo pode ser repetido quantas vezes desejar e também, é possível excluir ou modificar novamente as exceções existentes.

Utilizar as exceções também para a verificação em modo ocioso: Enquanto na verificação manual de vírus o computador é objetivamente verificado quanto a vírus e não deve ser utilizado para outras tarefas, a **Verificação em modo ocioso** é uma verificação inteligente de vírus, em que todos os arquivos do seu computador são sempre verificados se já não estão infectados com um vírus. A verificação em modo ocioso trabalha como um protetor de tela, sempre que o seu computador não estiver sendo usado, e para imediatamente assim que você continua a trabalhar para garantir um desempenho ideal. Aqui é possível estabelecer se, também para a verificação em modo ocioso, os arquivos de exceção ou os diretórios de exceção devem ser definidos.

Avançado

Um clique no botão **Avançado** possibilita efetuar configurações avançadas para a verificação de vírus. Na maioria dos casos, é totalmente suficiente utilizar as configurações padrão.

- **Tipos de arquivos**: Aqui é possível definir quais os tipos de arquivos em que o software deverá examinar a existência de vírus. A seleção da opção **Somente arquivos de programa e documentos** aumenta a velocidade.
- **Heurística**: Na análise heurística, os vírus não são reconhecidos somente por meio dos bancos de dados de vírus que você obtém a cada atualização do software antivírus mas também através de determinadas características típicas de vírus. Esse método é mais uma vantagem de segurança, no entanto, em raros casos, pode levar a um alarme falso.
- **Verificar pastas (compactadas)**: A verificação de dados em arquivos compactados (reconhecidos através das extensões de arquivo **ZIP**, **RAR** ou também **PST**) demanda muito tempo e normalmente pode ser ignorada quando a Sentinela de vírus estiver, em geral, ativada no sistema. Para aumentar a velocidade da verificação de vírus, você pode limitar o tamanho das pastas, que serão verificadas, para um determinado valor em megabytes.
- **Verificar pastas de e-mail**: Aqui é possível definir se também os seus arquivos de e-mail devem ser verificados quanto a infecções.
- **Verificar áreas do sistema**: As áreas de sistema (p.ex., setores de boot) do seu computador não devem ser ignoradas no controle de vírus.
- **Verificar Discador/Spyware/Adware/Riskware**: Com esta função, o seu sistema pode ser verificado também quanto a **Discadores** e outros softwares maliciosos (**Spyware**, **Adware** e **Riskware**). Aqui, trata-se de programas que estabelecem caras e indesejadas conexões à Internet e não ficam nada atrás dos vírus em relação ao seu potencial de dano comercial, que p.ex., armazenam secretamente o seu comportamento na navegação ou até mesmo todos os dados digitados (e com isso também suas senhas) e, na próxima oportunidade, encaminham através da Internet a terceiros.
- **Verificar a existência de Rootkits**: Os **Rootkits** tentam escapar dos métodos comuns de detecção de vírus. É sempre recomendável um controle adicional desses softwares maliciosos.
- **Verificar somente arquivos novos ou alterados**: Se você ativar esta função, serão verificados somente os arquivos que não são alterados há muito tempo e que antes tinham sido reconhecidos como inofensivos. Isso leva a um ganho de desempenho no trabalho diário – sem risco de segurança.
- **Criar relatório**: Neste campo de marcação, é possível definir se o software deve criar um registro sobre o processo de verificação de vírus. Isto pode ser visto na área **Registros**.

Atualizações

Se a atualização do software ou das assinaturas de vírus não funcionar pela internet, você pode fornecer todas as informações necessárias nesta área para possibilitar uma atualização automática. Informe aqui, nas opções, os seus dados de acesso (**nome de usuário** e **senha**) que você recebeu por e-mail no registro on-line do seu software. Com esses dados, você será reconhecido pelo servidor de atualização G Data e as atualizações podem ocorrer de forma completamente automática.

Se você adquiriu uma licença nova e quer ativá-la, selecione **Registrar no servidor**. As configurações da Internet mostram opções especiais que são necessárias apenas em alguns casos excepcionais (servidor proxy, outra região). Você deve ativar a verificação de versão apenas temporariamente quando tiver dificuldades na atualização das assinaturas de vírus.

Atualizar assinaturas de vírus automaticamente

Caso você não queira que o software G Data cuide da atualização das assinaturas de vírus automaticamente, você pode desmarcar a caixa aqui. No entanto, a desativação significa um alto risco de segurança e deve ser efetuada apenas em casos excepcionais. Se o intervalo entre as atualizações for muito pequeno para você, você pode adequá-lo individualmente e determinar, por exemplo, que estas sejam efetuadas apenas com o início da conexão à internet. Esta seleção faz sentido, por exemplo, em computadores que não têm uma conexão permanente com a internet.

Criar relatório: Se a marcação for colocada aqui, toda a atualização das assinaturas de vírus será integrada no registro, o que pode ser visualizado nas funções adicionais do software G Data (na **SecurityCenter** em **Mais** > **Registros**). Além desses registros, você encontra neles, por exemplo, informações sobre descobertas de vírus e outras ações que foram efetuadas pelo programa.

Registrar no servidor

Se você ainda não tiver registrado o seu software G Data poderá fazê-lo agora e inserir seu número de registro e os dados do cliente. Você encontra o **número de registro**, dependendo do tipo do produto, por ex., na contracapa do manual de utilização, no e-mail de confirmação no download do software ou na capa do CD.

Através da inserção do número de registro, o produto é ativado

Clique agora no botão **Log-in** e os seus dados de acesso serão gerados no servidor de atualização. Se o registro tiver sido realizado com sucesso, aparecerá uma tela de informações com a observação **O registro foi concluído com sucesso**, a qual pode ser fechada com o botão Fechar.

Atenção: Para a sua documentação e possíveis reinstalações do software, os seus **dados de acesso** também serão enviados por e-mail. Por isso, verifique se no seu registro on-line consta o seu endereço de e-mail correto, caso contrário, os dados de acesso não serão disponibilizados.

Para finalizar, os dados de acesso serão automaticamente aplicados na máscara de entrada original e então você poderá atualizar assinaturas de vírus através da Internet.

Não consegue se registrar no servidor? Se você não puder se registrar no servidor, talvez ele esteja em um servidor proxy. Clique no botão **Configurações da Internet**. Aqui será possível efetuar as configurações para sua conexão à Internet. Normalmente, em caso de problemas com a atualização das assinaturas de vírus, você deve primeiro verificar se consegue acessar a Internet com um navegador (por ex., Internet Explorer). Se você não conseguir criar uma conexão à internet, o problema provavelmente está na área da conexão à internet, e não nas informações do servidor proxy.

Configurações da Internet

Se utilizar um Servidor proxy, coloque a marcação em **Utilizar servidor proxy** Essas configurações só devem ser alteradas quando a atualização das assinaturas de vírus não funcionar. Se for necessário, fale com o administrador do sistema ou com o provedor de Internet sobre o endereço proxy. Se necessário, poderá inserir aqui os dados de acesso para o servidor proxy.

> **Servidor proxy**: Um servidor proxy junta consultas às redes e as distribui aos seus computadores conectados. Se utilizar o seu computador em uma rede da empresa, por exemplo, pode ser que você se conecte à rede através de um servidor proxy. Geralmente, em problemas com a atualização das assinaturas de vírus, você deverá verificar primeiramente se consegue se conectar à rede através de um servidor da internet. Se você não conseguir criar uma conexão à internet, o problema provavelmente está na área da conexão à internet, e não nas informações do servidor proxy.

Proteção da web

Aqui podem ser feitas as seguintes configurações.

- **Processar conteúdo da Internet (HTTP)**: Nas opções de proteção da Web, você pode definir que a existência de vírus em todo o **conteúdo da Web por HTTP** seja verificada já na navegação. O conteúdo infectado da Web não é executado e as respectivas páginas não são exibidas. Para isso, coloque a marcação em **Processar conteúdo da Internet (HTTP)**.

> Se você não desejar permitir a verificação dos conteúdos da Internet, **a sentinela de vírus** entra naturalmente em ação quando arquivos infectados forem executados. Ou seja, o seu sistema está protegido mesmo sem a verificação do conteúdo da Internet enquanto a sentinela estiver ativa.

> Você pode definir determinadas páginas da internet como exceções quando avaliá-las como inofensivas. Para isso, leia o capítulo **Definir exceções** Com o botão **Avançado**, você pode efetuar mais configuração sobre o tratamento de conteúdos da internet. Para os navegadores **Internet Explorer** e **Firefox**, existem plug-ins para efetuar as definições das exceções acima mencionadas diretamente no navegador, de forma mais confortável.

- **Proteção contra phishing:** Com os chamados **Phishing** os trapaceiros da Internet, tentam direcionar os clientes de um determinado banco ou loja, para um site falsificado e lá, roubar seus dados. O Filtro da Web recebe on-line e constantemente, as mais recentes informações sobre novos sites de phishing e os suprime automaticamente. A ativação dessa opção de Proteção contra phishing é altamente recomendada.
- **Enviar endereços de páginas da Internet infectadas**: Através desta função, você pode - naturalmente de forma anônima - informar automaticamente as páginas da Internet que foram consideradas como perigosas pelo software. Com isso você otimiza a segurança para todos os usuários.
- **Processar conteúdo de mensagens instantâneas**: Como vírus e outros programas maliciosos podem ser propagados também através de ferramentas de mensagens instantâneas, o software pode impedir a exibição e o download de dados infectados em primeiro plano. Se no aplicativo de mensagens instantâneas você não usar as portas padrão, poderá informar em **Avançado** as respectivas **portas**.
- **Inserção no aplicativo Messenger**: Se você utilizar o **Microsoft Messenger** ou o **Trillian**, é possível, colocando a marcação para o respectivo programa, definir um menu contextual no qual você poderá verificar a existência de vírus diretamente em arquivos suspeitos.

Definir exceções

Para colocar uma página da Internet como exceção na Whitelist, proceda da seguinte forma:

1. Clique no botão **Definir exceções**. A janela Whitelistserá exibida. Aqui serão exibidos os sites da web classificados como seguros e aqui inseridos.

2. Para adicionar outros sites da Internet, clique agora no botão Novo. Uma máscara de entrada será exibida. Em **URL**, insira o endereço do site (por exemplo, www.umsiteseguro.com.br) e, em **Comentário**, adicione uma nota, se necessário, descrevendo a razão de ter colocado o site. Confirme a inserção com um clique em OK.

3. Confirme então com um clique em OK todas as alterações feitas na Whitelist.

Para excluir novamente um site da whitelist, marque-o na lista com o mouse e clique no botão Para excluir.

Avançado

Aqui é possível definir quais **números de porta de servidor** devem ser monitorados pela proteção da Web. Normalmente, para um monitoramento do navegador normal, é suficiente aqui o número da porta 80.

- **Evitar ultrapassar limite de tempo no navegador**: Como o software processa o conteúdo da Internet antes de sua exibição no navegador da Internet, e esse, dependendo dos resultados dos dados necessita de um certo tempo, pode ocorrer que uma mensagem de erro apareça no navegador da Internet, pelo não recebimento imediato dos dados, devido a estarem sendo verificados. Com a colocação da marcação no campo **Evitar ultrapassar limite de tempo no navegador**, evita-se uma mensagem de erro e, assim que a existência de vírus for verificada em todos os dados do navegador, esses serão transmitidos normalmente para o navegador da Internet.

- **Limite de tamanho para downloads**: Através desta opção, é possível impedir uma verificação de HTTP para conteúdos da Web muito grandes. O conteúdo é verificado pela sentinela de vírus assim que qualquer rotina maliciosa ficar ativa. A vantagem dessa limitação de tamanho é de que ao navegar na Web, nenhum retardo ocorre devido ao controle de vírus.

Verificação de e-mail

Com a verificação de e-mail é possível verificar a existência de vírus em e-mails de entrada e saída, seus anexos e, desativar possíveis infecções diretamente na origem. Se um vírus for encontrado, o software é capaz de excluir diretamente anexos de arquivos ou reparar arquivos infectados.

No **Microsoft Outlook** a verificação de e-mail é realizada através de um **Plug-In**. Ele oferece a mesma proteção que as funções de proteção orientadas a **POP3/IMAP** dentro das opções do **AntiVirus**. Após a instalação desse Plug-in, você encontrará no menu do **Outlook**, **Ferramentas**, a função **Verificar individualmente a existência de vírus na pasta**, com a qual poderá verificar a existência de vírus em suas pastas de e-mail.

E-mails de entrada

- **No caso de uma infecção**: Aqui você pode definir o que deve ocorrer na detecção de um e-mail infectado. Dependendo do fim para o qual o seu computador é utilizado, diferentes configurações são recomendáveis. Por via de regra, a configuração **Desinfectar (se não for possível: excluir anexo/texto)** é a recomendada.
- **Verificar e-mails recebidos**: Com a ativação dessa opção, a existência de vírus é verificada em todos os **e-mails** que entram no computador durante o seu trabalho.
- **Verificar e-mails não lidos no início do programa (somente para o Microsoft Outlook)**: Essa opção serve para controlar a existência de vírus em e-mails que o acessam durante a sua conexão com a Internet. Portanto, assim que você abre o **Outlook**, todos os e-mails não lidos na pasta caixa de entrada e suas sub-pastas, serão controlados.
- **Anexar relatório aos e-mails recebidos e infectados**: Se tiver ativado a opção de relatório, aparecerá, em caso de uma detecção de vírus, na linha de assunto do e-mail infectado o aviso **VÍRUS** e, no começo do texto do e-mail, aparece a mensagem **Atenção! Este e-mail contém os seguintes vírus:** seguido pelo nome do vírus e a informação se o vírus foi excluído ou se o arquivo infectado pôde ser reparado.

E-mails de sada

- **Verificar e-mails antes do envio**: Para que você não encaminhe vírus inadvertidamente, o software oferece também a possibilidade de verificar a existência de vírus em seus e-mails antes do envio. Se você realmente desejar (inadvertidamente) enviar um vírus, aparece a mensagem **O e-mail [Linha de assunto] contém os seguintes vírus: [Virusname]**. O e-mail não pode ser enviado e o respectivo e-mail não será enviado.

Opções de varredura

- **Utilizar mecanismos:**: O software trabalha com dois mecanismos antivírus; duas unidades operacionais de análise independentes uma da outra. Em princípio, a utilização dos dois mecanismos é a garantia para os resultados ideais da profilaxia de vírus.

- **OutbreakShield**: Através dessa opção você ativa a OutbreakShield. O software cria, com a OutbreakShield ativada, somas de teste de e-mails, compara-as com as blacklists antispam constantemente atualizadas na Internet e, com isso, é capaz de reagir a um envio de e-mails em massa antes que existam as respectivas assinaturas de vírus. A OutbreakShield consulta na Internet sobre acumulações especiais de e-mails suspeitos e fecha, quase em tempo real, a brecha que existe entre o começo de um e-mail em massa e seu combate através de assinaturas de vírus adaptadas especialmente. A OutbreakShield está integrada no bloqueador de vírus de e-mail.

Avançado

Se na utilização do seu programa de e-mail você não usar as **portas padrão**, poderá informar em **Número da porta do servidor**, também a **porta** que utiliza para e-mails de entrada ou saída. Ao clicar no botão **Padrão**, é possível restaurar novamente e de forma automática o número da porta padrão. Você também pode inserir diversas portas. Separe-as respectivamente por uma vírgula.

O **Microsoft Outlook** é protegido por um Plugin especial, através do qual é possível diretamente do **Outlook** verificar pastas e e-mails. Para verificar a existência de vírus em um e-mail ou pasta no Outlook, selecione na barra de menu do Outlook o comando **Ferramentas > Verificar a existência de vírus na pasta** e a pasta de e-mail selecionada será verificada.

Como o software processa os e-mails de entrada oportunamente antes do próprio programa de e-mail, em grandes quantidades de e-mail ou conexões lentas, poderá aparecer uma mensagem de erro no programa de e-mail, pois esse não recebe imediatamente os dados dos e-mails que estão sendo verificados pelo software quanto a vírus. Com a ativação do campo de marcação em **Evitar ultrapassar limite de tempo no servidor de e-mail**, evita-se uma mensagem de erro do programa de e-mail e, assim que a existência de vírus for verificada em todos os dados de e-mails, esses serão encaminhados normalmente pelo software para o programa de e-mail.

Verificações automáticas de vírus

Aqui é possível ativar ou desativar a **Verificação em modo ocioso**. Além disso, você pode, em vez disso ou adicionalmente, examinar de forma periódica o seu computador ou as áreas do computador quanto a infecções. Por exemplo, você pode executar essas verificações nos períodos em que o seu computador não estiver sendo utilizado.

> **Verificações de vírus diferentes:** Em muitos casos, é suficiente quando o computador é verificado em modo ocioso. Com o botão **Novo**, você pode criar diferentes verificações automáticas de vírus e independentes entre si. Por exemplo, na pasta **Downloads**, você pode configurar que a sua coleção de MP3 seja verificada apenas uma vez por mês.

Geral

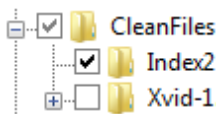
Aqui você determina o nome da verificação automática de vírus recentemente configurada. Para a diferenciação, recomenda-se nomes significativos, como por exemplo, **Discos rígidos locais (verificação semanal)** ou **Pastas (verificação mensal)**.

Se você colocar uma marcação em **Desligar o computador após a conclusão da tarefa**, o computador será desligado automaticamente após a conclusão da verificação automática de vírus. Isto é útil quando desejar, p. ex., executar a verificação de vírus após o trabalho no escritório.

> **Tarefa:** Cada uma das ordens automáticas definidas para a verificação do computador ou de determinadas áreas é denominada tarefa.

Escopo da análise

Defina aqui se a verificação de vírus deverá ser feita nos **Discos rígidos locais**, se as área **Memória** e **inicialização automática** devem ser testadas ou se deseja apenas verificar determinados **Diretórios** e **Arquivos**. Se for esse o caso, informe os diretórios desejados através do botão **Opção** .

> **Selecionar diretórios/arquivos**: Na árvore de diretórios (à esquerda), clicando nos sinais (+), é possível abrir e selecionar os diretórios cujo conteúdo será então exibido na visualização de arquivo. Cada diretório ou arquivo com uma marcação será verificado pelo software. Se nem todos os arquivos tiverem que ser verificados em um diretório, haverá uma marcação em cinza nesse diretório.

Programação

Nessa guia, é possível definir quando e em que ritmo a respectiva tarefa deverá ocorrer. Em **Executar**, insira uma predefinição que você pode detalhar em **Período**. Se você selecionar **Na inicialização do sistema**, as predefinições da programação continuarão e o Software executará a verificação sempre que o seu computador for reinicializado.

- **Executar a tarefa se o computador não estiver ligado na hora de início**: Com a ativação desta opção, as verificações automáticas de vírus não executadas serão feitas automaticamente assim que o computador for reinicializado.

- **Não executar com a bateria**: Para não reduzir a duração da bateria desnecessariamente, você pode, por ex., definir para **notebooks** que as verificações automáticas de vírus ocorram somente quando o computador portátil estiver conectado à rede elétrica.

Configurações de verificação

Nessa área você pode definir com que configurações a verificação automática de vírus deverá ocorrer.

- **Utilizar mecanismos**: O software trabalha com dois **mecanismos**, ou seja, dois programas de verificação independentes entre si. Cada mecanismo, por si só, já protegeria contra vírus, em alta escala, mas, exatamente a combinação de ambos os mecanismos, oferece os melhores resultados. Em computadores antigos e lentos, é possível, mediante a utilização de apenas um único mecanismo, acelerar a verificação de vírus; no entanto, via de regra, deve-se manter a configuração **Ambos os mecanismos**.
- **Arquivos infectados**: O software encontrou um vírus? Na configuração padrão, o software pergunta o que você deseja fazer com o vírus e o arquivo infectado. Quando desejar executar sempre a mesma ação, poderá definir isto aqui. A máxima segurança para os seus dados é oferecida pela configuração **Desinfectar (se não for possível: para quarentena) quarentena))**.
- **Pastas infectadas**: Defina aqui se a **pasta** (por exemplo, arquivos com a extensão **RAR**, **ZIP** ou também **PST**) deverão ser tratados de forma diferente dos arquivos normais. No entanto, observe que mover um arquivo compactado para a quarentena pode danificá-lo, de forma que ele também não poderá mais ser usado após movê-lo de volta. Por essa razão, em caso de pastas infectadas, recomenda-se decidir caso a caso e selecionar **Perguntar as ações desejadas**.

Além disso, defina através do clique no botão **Avançado** que verificações adicionais deverão ser executadas pelas verificações de vírus adicionais.

Na maioria dos casos, é totalmente suficiente utilizar as configurações padrão.

- **Tipos de arquivos**: Aqui é possível definir quais os tipos de arquivos em que o software deverá examinar a existência de vírus.
- **Heurística**: Na análise heurística, os vírus não são reconhecidos somente por meio dos bancos de dados de vírus que você obtém a cada atualização do software, mas também através de determinadas características típicas de vírus. Esse método é mais uma vantagem de segurança, no entanto, em raros casos, pode levar a um alarme falso.

- **Verificar pastas (compactadas)**: A verificação de dados em arquivos compactados (reconhecidos através das extensões de arquivo **ZIP**, **RAR** ou também **PST**) demanda muito tempo e normalmente pode ser ignorada quando a **Sentinela de vírus** estiver, em geral, ativada no sistema. Ela reconhece na descompactação um vírus oculto até o momento e, impede automaticamente a sua propagação.
- **Verificar pastas de e-mail**: Aqui é possível definir se também os seus arquivos de e-mail devem ser verificados quanto a infecções.
- **Verificar áreas do sistema**: As áreas de sistema (p.ex., **setores de boot**) do seu computador não devem ser ignoradas no controle de vírus.
- **Verificar Discador/Spyware/Adware/Riskware**: Com esta função, o seu sistema pode ser verificado também quanto a **Discadores** e outros softwares maliciosos (**Spyware**, **Adware** e **Riskware**). Aqui, trata-se de programas que estabelecem caras e indesejadas conexões à Internet e não ficam nada atrás dos vírus em relação ao seu potencial de dano comercial, que p.ex., armazenam secretamente o seu comportamento na navegação ou até mesmo todos os dados digitados (e com isso também suas senhas) e, na próxima oportunidade, encaminham através da Internet a terceiros.
- **Verificar a existência de Rootkits**: Os **Rootkits** tentam escapar dos métodos comuns de detecção de vírus. É sempre recomendável um controle adicional desses softwares maliciosos.
- **Criar relatório**: Neste campo de marcação, é possível definir se o software deve criar um registro sobre o processo de verificação de vírus. Isto pode ser visto na área **Registros**.

Conta do usuário

Aqui é possível inserir a conta de usuário na qual a verificação de vírus deverá ocorrer. Essa conta será necessária para o acesso à unidade de rede.

Firewall

Além do modo Piloto automático, para muitos usuários provavelmente a melhor escolha, você ainda tem muitas opções para configurar o firewall G Data de forma ideal conforme as suas necessidades e exigências.

> Se você quiser levantar a temática do firewall intensivamente, o capítulo **Operação do firewall** Informações avançadas

Automático

Nas configurações do firewall, existem duas áreas básicas que podem ser configuradas individualmente:

Modo

Aqui é possível definir se o firewall atua de maneira automática e autodidata, e se o usuário não é questionado na decisão sobre o bloqueio ou a liberação de consultas da Internet ou se o usuário é consultado em caso de dúvidas e vinculado na criação de novas regras de firewall através de consulta.

- **Modo Piloto automático**: Aqui o Firewall trabalha de forma totalmente autônoma e evita os perigos automaticamente de PCs residenciais. Essa configuração oferece uma proteção geral prática e é, na maioria dos casos, recomendável.
- **Criação manual de regras**: Se desejar configurar seu firewall individualmente, através da criação manual de regras você poderá ajustar a proteção de firewall totalmente às suas necessidades pessoais.
- **Oferecer o modo de piloto automático quando um aplicativo de tela cheia for iniciado**: Principalmente em **jogos de computadores** (e outros **aplicativos de tela cheia**), pode ser perturbador quando o firewall interrompe o fluxo do jogo com muitas consultas ou simplesmente perturba a exibição. Para poder garantir a diversão no jogo sem interrupções e sem abrir mão da segurança, o piloto automático é uma configuração útil que suprime as consultas do firewall. Se o piloto automático não for utilizado como configuração padrão, esta função pode cuidar para que ele seja sempre oferecido quando você usa um programa que é executado no **modo tela cheia**.

Configuração de segurança

Enquanto você utiliza o computador para o seu trabalho diário, o Firewall aprende cada vez mais que programas você utiliza para o acesso à Internet e que programas são ou não um risco para a segurança. A vantagem da utilização de níveis de segurança predefinidos é que, mesmo sem esforços administrativos e conhecimentos técnicos na área de segurança de rede, o firewall pode ser adaptado às necessidades individuais. Para isso, basta definir com o ajuste deslizante o nível de segurança desejado. Como opção, existem os seguintes níveis de segurança:

- **Segurança máxima**: as regras do Firewall são criadas com diretrizes de granularidade muito finas. Para isso, é necessário ter conhecimentos sobre a terminologia específica de redes (TCP, UDP, portas etc.). O firewall detecta as inconsistências e você será questionado frequentemente durante a fase de aprendizado.
- **Segurança alta**: as regras do Firewall são criadas com diretrizes de granularidade muito finas. Para isso, é necessário ter conhecimentos sobre a terminologia específica de redes (TCP, UDP, portas e etc.). O firewall questionará freqüentemente durante a fase de aprendizado em determinadas circunstâncias.
- **Segurança normal**: as regras do Firewall são criadas somente no nível do aplicativo. Os assistentes não consultarão o usuário sobre os detalhes específicos de rede. Você é solicitado o menos possível durante a fase de aprendizado.
- **Segurança baixa**: as regras do Firewall são criadas somente no nível do aplicativo. Os assistentes mantêm os detalhes específicos de rede longe de você. Você é pouco solicitado durante a fase de aprendizado. Neste nível de segurança, existe também a máxima proteção de segurança contra solicitações de conexão.
- **Firewall desativado**: O firewall pode ser desativado se for necessário. O seu computador estará ainda conectado à Internet e a outras redes, mas não estará protegido contra ataques ou espionagem.

Se desejar configurar o firewall de forma mais específica, coloque a marcação em **Segurança definida pelo usuário (para usuários experientes)**. No entanto, observe que para essas configurações é necessário ter pelo menos um conhecimento básico sobre segurança de redes.

Consultas

Defina aqui quando, como e se um firewall deverá consultar o usuário assim que programas solicitarem o estabelecimento de uma conexão com a Internet ou rede.

- **Criar regra**: Quando o firewall detecta a aceitação de uma conexão com a rede, aparece uma caixa de informações onde você define como deve ser procedido com o respectivo aplicativo. Aqui é possível definir o que exatamente você deseja determinar com a permissão ou proibição de um acesso à rede:

Por aplicativo: Aqui, o acesso à rede para o aplicativo exibido no momento é permitido ou recusado em geral para todas as portas e como todos os protocolos de transmissão (**TCP** ou **UDP**).

Por registro/porta/aplicativo: O aplicativo que solicitar um acesso à rede receberá a permissão apenas com o protocolo de transmissão e para se conectar exclusivamente com a porta solicitada. Se o mesmo aplicativo solicitar um outro acesso à rede em uma outra porta ou com um outro registro, aparecerá novamente a Consulta, e uma outra regra relacionada a isso poderá ser criada.

Por aplicativo, se no mín. __ consultas estão na fila: Existem aplicativos (como o Microsoft Outlook) que em uma solicitação de rede, consultam ao mesmo tempo diversas portas ou utilizam ao mesmo tempo diferentes registros. Como isso significaria diversas consultas, p.ex., na configuração **Por registro/porta/aplicativo**, é possível definir aqui, que os aplicativos recebam uma liberação ou recusa generalizada para utilização da rede, assim que a conexão for permitida ou recusada pelo usuário.

- **Aplicativos de servidor desconhecidos**: Aplicativos que ainda não são gerenciados através de uma regra no firewall, podem ser tratados de diferentes formas. O momento da consulta permanece aqui de certa forma suposto. Quando o servidor de aplicativo entra **Em recepção**, isso significa que ele espera quase em standby uma solicitação de conexão. Caso contrário, a consulta acontece apenas quando se faz a própria solicitação da conexão.
- **Verificação quanto a redes desprotegidas**: Naturalmente, um firewall só pode funcionar sem problemas quando todas as redes que o computador a ser protegido acessa, também possam ser reconhecidas e monitoradas. Por isso, essa verificação quanto a redes desprotegidas deveria permanecer obrigatoriamente ativada.
- **Repetir consultas de aplicativos**: Você pode vincular Solicitações de conexão repetidas a um aplicativo. Dessa forma, em tentativas de conexão que ainda não foram especificadas através de uma regra, não aparece constantemente uma consulta, mas apenas em intervalos de 20 segundos ou um outro intervalo definível por você.

Verificação de referência

Na verificação de referência, é apurada, para aplicativos aos quais o firewall já permitiu o acesso à rede, uma soma de testes com base no tamanho do arquivo e outros critérios. Quando essa soma de teste repentinamente difere do programa, pode ser devido ao fato do programa ter sido alterado por um programa malicioso. Nesse caso, o firewall dá um alarme.

A **verificação de referência para módulos carregados** observa da mesma forma os **módulos** que os aplicativos utilizam (por ex., DLLs). Como esses se modificam frequentemente ou novos módulos são carregados posteriormente, uma verificação consequente de referências modificadas e desconhecidas em módulos pode levar a um esforço considerável na utilização do firewall. Cada módulo alterado tornaria necessária uma consulta de segurança do firewall. Portanto, a verificação de módulos só deve ser utilizada dessa forma, em demandas muito altas à segurança.

Outros

Aqui estão disponíveis outras possibilidades de configuração.

- **Configurações padrão para o assistente de regras**: Aqui é possível definir se a criação de novas regras será executada através do **Assistentes de regras** ou na **caixa de diálogo avançado**. Para os usuários que não têm conhecimento sobre o assunto Segurança de rede, recomendamos o **Assistente de regras**.
- **Verificações na inicialização do programa**: Aqui você pode definir se o firewall deve procurar por **aplicações desconhecidas do servidor** a cada inicialização do programa. Esta função de busca deve ser ativada sempre, exceto se você trabalhar em uma rede fechada.
- **Salvar registro de conexão**: Aqui você pode definir quanto tempo o firewall deve manter os dados de conexão. Os dados podem ser mantidos entre uma a 60 horas e visualizados na área do programa do firewall. **Registro** visualizar.

Anti-spam

Aqui é possível definir configurações básicas para o tratamento de e-mails de spam.

Filtro de spam

Através do filtro de spam, você tem amplas possibilidades de configuração para bloquear de forma eficaz os e-mails com conteúdo ou remetentes indesejados (por ex., remetentes de e-mail em massa). O programa verifica diversas características típicas de spam nos e-mails. Com o auxílio das características correspondentes, é calculado um valor que espelha a possibilidade de Spam. Aqui, por meio do botão **Utilizar filtro de spam**, você ativa ou desativa o filtro de spam. Para ativar ou desativar os diferentes tipos de filtragem do filtro de spam, coloque ou remova a marcação do respectivo registro. Para fazer alterações nos diferentes filtros, basta clicar no respectivo registro. Uma janela de diálogo aparecerá em seguida, na qual as respectivas configurações podem variar. As seguintes possibilidades de configuração estão disponíveis:

- **Spam-OutbreakShield**: Com o **OutbreakShield**, é possível o reconhecer e combater pragas em e-mails em massa antes que as assinaturas de vírus atualizadas estejam disponíveis. O OutbreakShield consulta na Internet sobre acumulações especiais de e-mails suspeitos e fecha, quase em tempo real, a brecha que existe entre o começo de um e-mail em massa e seu combate através de assinaturas de vírus adaptadas especialmente.

  Se utilizar um computador atrás de um Servidor proxy, clique no botão **Configurações da Internet** e faça as respectivas alterações. Essas configurações só devem ser alteradas quando a OutbreakShield não funcionar.

- **Whitelist**: Através da Whitelist você pode excluir determinados endereços de remetentes ou domínios, explicitamente da suspeita de spam. Para isso, basta inserir no campo **Endereços/Domínios** o endereço de e-mail desejado (por ex., newsletter@gdata.de) ou o domínio (por ex., informationsseite.de) que deseja excluir da suspeita de spam e o software G Data não tratará e-mails desse remetente ou do domínio remetente como spam. Através do botão **Importar**, você também pode adicionar listas prontas de endereços de e-mails ou domínios na Whitelist. Os endereços e domínios deverão estar um abaixo do outro em linhas individuais na lista. Como formato, é utilizado um arquivo simples em txt que pode ser criado também com o Windows Notepad. Através do botão **Exportar**, você também pode exportar uma Whitelist como arquivo de texto.

- **Blacklist**: Através da Blacklist, você pode colocar determinados endereços de remetentes ou domínios explicitamente em suspeita de spam. Para isso, basta inserir no campo **Endereços/Domínios** o endereço de e-mail desejado (por ex., newsletter@megaspam.de.vu) ou o domínio (p.ex., megaspam.de.vu) que deseja colocar em suspeita de spam e o software G Data tratará e-mails desse remetente ou do domínio remetente em geral como e-mails com altíssima probabilidade de spam. Através do botão **Importar**, você também pode adicionar listas prontas de endereços de e-mails ou domínios na Blacklist. Os endereços e domínios deverão estar um abaixo do outro em linhas individuais na lista. Como formato, é utilizado um arquivo simples em txt que pode ser criado também com o Windows Notepad. Através do botão **Exportar**, você também pode exportar uma Blacklist como arquivo de texto.

- **Utilizar blacklists em tempo real**: Na Internet, existem listas negras que contêm endereços IP de servidores, através dos quais spams são enviados. O software G Data apura, através de Consultas de DNS nas Realtime Blacklists (blacklists em tempo real), se o servidor que envia está listado. Caso afirmativo, aumenta a Probabilidade de spam. Em geral, deve-se utilizar aqui a configuração padrão, no entanto, é possível inserir também em Blacklist 1, 2 e 3 e endereços próprios para listas negras da Internet.

- **Utilizar palavras-chave (texto do e-mail)**: Com a lista de **palavras-chave**, você pode, mediante ajuda das palavras utilizadas no **texto do e-mail**, colocar e-mails em suspeita de spam. Quando pelo menos um dos termos no texto do e-mail aparecer, aumenta a probabilidade de spam.

Essa lista pode ser alterada como desejado, através dos botões **Adicionar**, **Alterar** e **Excluir**. Com o botão **Importar**, você também pode inserir listas de palavras-chave preparadas em sua lista. Os registros deverão estar um abaixo do outro em linhas individuais na lista. Como formato, é utilizado um arquivo simples em txt que pode ser criado também com o Windows Notepad. Através do botão **Exportar**, você também pode exportar uma lista de palavras-chave como arquivo de texto. Através da marcação **Pesquisar somente palavras completas** é possível definir que o software G Data só pesquise por palavras inteiras na linha de assunto de um e-mail. Assim, p.ex., um termo como **pica** cairia sob suspeita de spam, enquanto que o termo desejado **Picasso** permaneceria incontestado.

- **Utilizar palavras-chave (assunto)**: Com a lista das palavras-chave, você pode, mediante ajuda das palavras utilizadas na linha de assunto, colocar e-mails em suspeita de spam. Quando pelo menos um dos termos na linha de assunto aparecer, aumenta a probabilidade de spam.

- **Utilizar filtro de conteúdo**: O **Filtro de conteúdo** é um filtro autodidata que calcula, de acordo com as palavras utilizadas no texto do e-mail, uma probabilidade de spam. Esse filtro trabalha não somente com base em listas de palavras existentes, mas aprende com cada novo e-mail recebido. Com o botão **Consultar conteúdo da tabela**, é possível solicitar as listas de palavras que o filtro de conteúdo utiliza para classificar um e-mail como spam. Com o botão **Redefinir tabela**, você exclui todo o conteúdo aprendido da tabela, e o filtro de conteúdo autodidata começa novamente o processo de aprendizado.

Reação

Aqui você pode determinar como o filtro de spam deve tratar os e-mails que possivelmente contêm spam. Nesse processo, é possível definir três níveis, que podem ser influenciados pelo nível de probabilidade que o softwareG Data utiliza para isso, já que se trata de spam no e-mail afetado.

- Em **Suspeita de spam**, é regulada a manipulação de e-mails nos quais o software G Data encontra elementos de spam individuais. Aqui geralmente pode não se tratar de spam, mas, em alguns casos raros de e-mails com boletins informativos ou e-mails conjuntos totalmente desejados pelo destinatário. Recomenda-se aqui indicar o destinatário sobre a suspeita de spam.

- Em **Alta probabilidade de spam**, são reunidos os e-mails que contêm as diversas características de spam e somente em raríssimos casos são realmente desejados pelo destinatário.
- Em **Altíssima probabilidade de spam**, encontram-se os e-mails que atendem a todos os critérios de um spam. Aqui, quase nunca se trata de e-mails desejados e a rejeição desse tipo de e-mail é na maioria das vezes recomendável.

Cada uma dessas reações com três níveis podem ser configuradas individualmente. Para isso, basta clicar no botão **Alterar** e definir a reação que o software G Data deve ter. Assim, em **Rejeitar e-mail**, você tem a possibilidade de que o e-mail nem chegue a entrar em sua caixa de entrada. Em **Inserir aviso de spam no assunto** e **Inserir texto do e-mail**, você pode marcar e-mails identificados como spam de forma chamativa, para poder organizá-los melhor, por exemplo. Se utilizar o **Microsoft Outlook** (atenção: não confundir com o **Outlook Express** ou o **Windows Mail**), existe também a possibilidade de mover os e-mails com suspeita de spam para uma pasta livremente definível em sua caixa postal (**Mover e-mail para a pasta**). Essa pasta pode ser criada diretamente através do software G Data , definindo a respectiva pasta em **Nome da pasta**.

Mesmo se não utilizar o **Outlook**, você poderá mover os e-mails reconhecidos como spam para uma **Pasta**. Para isso, insira um aviso na linha de assunto (por ex., "[Spam]") e crie em seu programa de e-mail uma regra que mova os e-mails com o texto na linha de assunto para uma outra pasta.

Configurações avançadas

Nesta área, você pode modificar o reconhecimento de spam do softwareG Data muito detalhadamente e adequá-lo às condições de seu tráfego de e-mails. No entanto, recomenda-se em geral, utilizar as configurações padrão. Nas configurações avançadas, você só deve efetuar alterações quando tiver conhecimentos sobre o assunto e souber exatamente o que faz.

Outros

Nesta área você tem a possibilidade de efetuar outras configurações.

- **Verificar e-mails não lidos na caixa de entrada na inicialização do programa**: Somente para o **Microsoft Outlook**: Esta opção serve para verificar os e-mails sob suspeita de spam. Assim que você abrir o **Outlook**, todos os e-mails não lidos na pasta da caixa de entrada e das subpastas integradas são verificados pelo softwareG Data.
- **Outros programas de e-mail (utilização de POP3)**: E-mails recebidos por **POP3** não podem ser excluídos diretamente por razões técnicas. Se um filtro tiver de rejeitar e-mails, esse e-mail receberá um texto de substituição padrão. O texto de substituição de e-mails rejeitados é o seguinte: **A mensagem foi rejeitada**. No entanto, o texto para essas funções de notificação podem ser editados individualmente. No texto a ser definido livremente para o assunto e o texto do e-mail, são disponibilizados os seguintes **espaços reservados** (definido por um sinal de percentual seguido por uma letra minúscula):

%s	Remetente
%u	Assunto

No seu programa de e-mail, você pode definir uma regra que exclui automaticamente os e-mails com o texto de substituição aqui definido.

Outros filtros

Os seguintes filtros são configurados, por padrão, mas também podem ser desativados, em caso de necessidade, bastando remover a marcação.

- **Desativar scripts HTML**
- **Filtrar anexos perigosos**

Para isso, através do botão **Novo**, você pode criar novas regras de filtro ou, através do botão **Editar**, editar os filtros existentes. Os filtros criados são exibidos na lista e podem ser ativados ou desativados conforme desejado na marcação à esquerda do respectivo registro. Quando houver uma marcação no campo da marcação, o respectivo filtro está ativo. Quando não houver uma marcação no campo, o respectivo filtro não está ativo. Para excluir o filtro permanentemente, selecione-o com um clique do mouse e utilize em seguida o botão **Excluir**.

> As opções de filtro disponíveis aqui são filtros adicionais que suportam o filtro de spam do software G Data e simplificam as configurações individuais. Através do próprio filtro de spam, você tem amplas possibilidades de configuração para bloquear de forma eficaz os e-mails com conteúdo ou remetentes indesejados (por ex., remetentes de e-mail em massa). O programa verifica diversas características típicas de spam nos e-mails. Com o auxílio das características correspondentes, é calculado um valor que espelha a possibilidade de Spam. Para isso, estão disponíveis diversas guias nas quais todas as possibilidades de configuração são disponibilizadas e estruturadas de forma temática.

Quando um novo filtro é criado, uma janela de opções é aberta onde é possível definir o **tipo de filtro** básico. Todos os outros dados para o filtro a ser criado podem ser inseridos em uma janela assistente apropriada. Dessa forma, você cria confortavelmente filtros contra todos os tipos de perigo.

- **Desativar scripts HTML**: Esse filtro desativa **scripts** na parte **HTML** de um e-mail. Scripts que possam ter um sentido em uma página da Internet são bastante perturbadores quando estão anexados em um e-mail em HTML. Em alguns casos, os scripts HTML são utilizados ativamente para infectar arquivos nos quais os scripts têm a possibilidade de não se propagar apenas com a abertura de um anexo infectado, mas por si só podem ter efeito já na **pré-visualização** de um e-mail.

- **Filtrar anexos perigosos**: Ao filtrar anexos, você tem muitas possibilidades para filtrar anexos de e-mail. A maioria dos vírus de e-mails se propaga através desses tipos de anexos que, em sua maioria, contêm arquivos executáveis bem ou mal escondidos. Eles podem incluir um arquivo exe clássico, que contém um programa malicioso, ou também scripts VB que se esconde sob determinadas pré-condições ou até mesmo em arquivos presumidamente seguros de gráficos, filmes ou música. Em geral, todos os usuários devem ser extremamente cuidadosos na execução de anexos de e-mail e, em caso de dúvidas, é melhor consultar novamente o remetente do e-mail antes de executar um arquivo que não foi explicitamente solicitado. Em **Extensões de arquivos** , é possível listar as extensões de arquivos para as quais os respectivos filtros devem ser aplicados. Assim, é possível, por exemplo, reunir todos os arquivos executáveis (como arquivos exe e com) em um filtro mas também filtrar outros formatos (como MPEG, AVI, MP3, JPEG, JPG, GIF, etc,) quando estes representarem uma sobrecarga para o servidor de e-mails devido ao seu tamanho. É claro que é possível também filtrar **pastas compactadas** (como ZIP, RAR ou CAB). Separe todas as extensões de arquivo de um grupo de filtros por **ponto e vírgula**. Por meio da função **Filtrar também os anexos em e-mails incorporados**, você faz com que a filtragem dos tipos de anexos selecionados em **Extensões de arquivo** seja feita também em e-mails que representem, por si só, um anexo de um e-mail. Essa opção deve ser ativada em geral. Em **Somente renomear anexos**, os anexos a serem filtrados não são excluídos automaticamente, mas apenas renomeados. Isso é bastante útil por exemplo, em arquivos executáveis (como EXE e COM) mas, também em **arquivos do Microsoft Office** que possivelmente possam conter scripts executáveis e macros. Ao **renomear** um anexo, ele não pode ser aberto inadvertidamente com um clique do mouse, pois deve ser salvo e, se necessário, renomeado antes que possa ser utilizado. Quando a marcação em **Somente renomear anexos** não estiver presente, os respectivos anexos são excluídos diretamente. Em **Sufixo**, você informa a sequência de caracteres desejada com a qual você deseja que a extensão do arquivo seja ampliada, evitando, assim, a executabilidade de um arquivo através de um simples clique (por ex., exe_danger). Em **Inserir aviso no texto do e-mail**, é possível informar ao destinatário do e-mail filtrado que um anexo foi excluído ou renomeado devido à regra de filtragem.

- **Filtro de conteúdo**: Através do filtro de conteúdo é possível bloquear de forma confortável, e-mails que contenham determinados tópicos ou textos. Para isso, em **Critério de pesquisa**, insira as **palavras-chave** e as **expressões** às quais o softwareG Data deverá reagir. Nesse processo, é possível vincular o texto da forma desejada com operadores lógicos **E** e **OU** Agora, digite em **Área de pesquisa** em que área de um e-mail os termos devem ser procurados. Como **Cabeçalho** é denominada a área de um e-mail que, entre outras coisas, contém o endereço de e-mail do remetente e do destinatário, a linha de assunto e as informações sobre os programas utilizados, protocolos e dados do remetente. E ao contrário, com **Assunto**, só é verificado o conteúdo da linha de assunto sem outras informações do texto do cabeçalho. Em **Texto do e-mail** você tem, além disso, a opção se a área de pesquisa deve limitar-se apenas a simples **e-mails com texto** ou abranger também o texto em **e-mails em HTML** (Texto HTML). Em **E-mails incorporados**, você pode definir se a procura do filtro de conteúdo deverá englobar também os que estejam presentes como anexo no e-mail recebido. Em **Reação**, é possível definir como deve ser o procedimento com e-mails reconhecidos pelo software G Data como spam. Em **Rejeitar e-mail**, o respectivo e-mail não é nem recebido pelo seu programa de e-mail; quando você colocar uma marcação em **Inserir aviso no assunto e texto do e-mail**, será possível colocar um aviso no próprio texto e na linha de assunto (**prefixo na linha de assunto**), p.ex., **Spam** ou **Atenção**. Opcionalmente, também é possível inserir um texto que precederá o texto do próprio e-mail (**Aviso no texto**). Se utilizar o **Microsoft Outlook** (atenção: Não confundindo com o **Outlook Express** ou o **Windows Mail**), existe também a possibilidade de mover os e-mails com suspeita de spam para uma pasta livremente definível em sua caixa postal (**Mover e-mail para a pasta**). Essa pasta pode ser criada diretamente através do software G Data , definindo a respectiva pasta em **Nome da pasta**.

O operador lógico **E** tem como pré-requisito que todos os elementos vinculados com E estejam presentes e, o operador **OU**, apenas que um elemento esteja presente.

- **Filtro de remetente**: Através do filtro de remetente é possível bloquear de forma confortável e-mails de determinados remetentes. Para isso, basta inserir em **Remetente/Domínios** os **endereços de e-mail** ou os **nomes de domínios** aos quais o software G Data deverá reagir. Diversos registros podem ser separados através de **ponto e vírgula**. Em **Reação**, é possível definir como deve ser o procedimento com e-mails reconhecidos pelo software G Data como spam. Em **Rejeitar e-mail**, o respectivo e-mail não é nem recebido pelo seu programa de e-mail; quando você colocar uma marcação em **Inserir aviso no assunto e texto do e-mail**, será possível colocar um aviso no próprio texto e na linha de assunto (**prefixo na linha de assunto**), p.ex., **Spam** ou **Atenção**. Opcionalmente, também é possível inserir um texto que precederá o texto do próprio e-mail (**Aviso no texto**). Se utilizar o **Microsoft Outlook** (atenção: não confundir com o **Outlook Express** ou o **Windows Mail**), existe também a possibilidade de mover os e-mails com suspeita de spam para uma pasta livremente definível em sua caixa postal (**Mover e-mail para a pasta**). Essa pasta pode ser criada diretamente através do software G Data , definindo a respectiva pasta em **Nome da pasta**.

- **Filtro de idioma**: Com o Filtro de idioma, você pode definir e-mails em determinados idiomas automaticamente como spam. Se, por via de regra, você não tiver nenhum contato por e-mail com uma pessoa do idioma inglês, pode filtrar muitos spams através da definição do inglês como **Idioma de spam**. Selecione o idioma do qual você supõe normalmente não receber nenhum e-mail e, o software G Data aumenta com isso significativamente a avaliação de spam para esses e-mails. Em **Reação**, é possível definir como deve ser o procedimento com e-mails reconhecidos pelo software G Data como spam. Em **Rejeitar e-mail**, o respectivo e-mail não é nem recebido pelo seu programa de e-mail; quando você colocar uma marcação em **Inserir aviso no assunto e texto do e-mail**, será possível colocar um aviso no próprio texto e na linha de assunto (**prefixo na linha de assunto**), p.ex., **Spam** ou **Atenção**. Opcionalmente, também é possível inserir um texto que precederá o texto do próprio e-mail (**Aviso no texto**). Se utilizar o **Microsoft Outlook** (atenção: não confundir com o **Outlook Express** ou o **Windows Mail**), existe também a possibilidade de mover os e-mails com suspeita de spam para uma pasta livremente definível em sua caixa postal (**Mover e-mail para a pasta**). Essa pasta pode ser criada diretamente através do software G Data , definindo a respectiva pasta em **Nome da pasta**.

Otimizador

Aqui você pode alterar configurações básicas do software. Para isso, clique na guia com a respectiva opção de configuração.

Geral

Aqui é possível efetuar as seguintes configurações:

- **Excluir dados de restauração**: Aqui você pode definir quando os **dados de restauração** (que o software G Data cria nas alterações) deverão ser excluídos.
- **Excluir dados antigos**: Aqui você pode definir quando dados antigos (por ex., pastas temporárias antigas) deverão ser excluídos.
- **Excluir vinculações da área de trabalho**: Aqui você pode definir quando **vinculações da área de trabalho** desnecessárias (quando não tiverem sido utilizadas por um determinado número de dias) deverão ser excluídas.
- **Nas atualizações da Microsoft, procurar também por atualizações do Office**: Aqui é possível definir se o Otimizador deve procurar automaticamente na Internet além dos atuais **Windows Updates** também por **atualizações do Office**. Uma atualização de ambos os elementos economiza tempo e mantém você no estado mais atual do ponto de vista técnico de segurança.

  Naturalmente, a procura por atualizações do Office funciona apenas quando o Microsoft Office estiver instalado no respectivo computador.

- **Não criar nenhum arquivo de registro detalhado sobre elementos excluídos:** O otimizador é estruturado de forma a registrar informações completas sobre as alterações executadas. Se você considerar um risco de segurança um arquivo de registro com as respectivas informações sobre o que o Otimizador excluiu, é possível impedir a criação desse tipo de registro de exclusão.
- **Excluir permanentemente os arquivos temporários:** Com essa função, você fecha os arquivos da Web (por ex., cookies, arquivos temporários da Internet) da opção de restauração do Otimizador, ou seja, não poderá mais restaurar esses arquivos.

Ao ativar essa função, você reduz substancialmente a quantidade de arquivos que o Otimizador tem que administrar na área **Restaurar**. Isso melhora o desempenho.

- **Não permitir a reinicialização automática do computador através do serviço:** Com essa opção, você impede uma possível **reinicialização do computador** eventualmente executada pelo Otimizador em um procedimento de otimização controlada por tempo. Como uma reinicialização do computador sem a consulta pelo Otimizador só seria executada se nenhum usuário estivesse conectado, na maioria dos casos, seria recomendável não ativar essa opção.
- **Permitir restauração de pontos de restauração individuais:** Sem esta função, o software G Data não pode mais executar nenhuma restauração.

Configuração

Na área **Configuração** você pode selecionar todos os módulos que o Otimizador deverá utilizar para um processo de otimização. Os módulos selecionados serão iniciados através de uma ação automática controlada por tempo (consulte o capítulo **Programação**) ou manualmente. Para ativar o módulo, dê um clique duplo com o mouse no módulo. Aqui você pode otimizar individualmente as seguintes grandes áreas de configuração:

- **Segurança**: Diversas funções que carregam automaticamente os dados da Internet, só têm aspectos úteis para o fornecedor e não para o usuário. Muitas vezes, são abertas portas e portões para software malicioso através dessas funções. Com esses módulos, você protege o seu sistema e o mantém no estado mais atual.
- **Desempenho**: Arquivos temporários, p.ex., cópias de segurança não mais necessárias, arquivos de registro ou dados de instalação que após a instalação só ocupam espaço, freiam o seu disco rígido e ocupam valioso espaço de armazenamento. Além disso, processos não mais necessários e vínculos de arquivos diminuem incrivelmente a velocidade do seu sistema. Com os módulos aqui relacionados, você pode liberar o seu computador dessa carga desnecessária e ganhar velocidade.
- **Proteção de dados**: Aqui estão reunidos os módulos que lidam com a proteção dos seus dados. Aqui serão excluídos os rastros criados involuntariamente através da navegação ou da utilização geral do computador, e que revelam muito sobre o seu comportamento de usuário e, até mesmo dados importantes e senhas.

Proteção de pastas

Por meio dessa guia você pode retirar determinadas pastas (p.ex., também a sua **partição do Windows**) da exclusão automática de arquivos antigos.

Para isso, clique simplesmente no símbolo Adicionar e selecione a respectiva pasta ou a unidade desejada.

Para liberar novamente um Diretório de exceções selecione o da lista visualizada e, em seguida, clique no botão **Excluir**.

Proteção de arquivos

Com a proteção de arquivos, é possível proteger determinados arquivos da exclusão pelo otimizador, p.ex., **status de jogos para computador** ou arquivos semelhantes com extensões de arquivo incomuns, que podem ser interpretados como arquivos de backup ou temporários.

Para proteger arquivos específicos, clique no botão Adicionar e digite o respectivo nome do arquivo. Aqui também é possível trabalhar com espaços reservados.

A forma de funcionamento dos **Espaços reservados** é a seguinte:

- O **ponto de interrogação** (?) é substituto para caracteres individuais.
- * O **asterisco** (*) é substituto para seqüências de caracteres inteiras.

Para, por exemplo, proteger todos os arquivos com a extensão **.sav** , digite ***.sav**. Para verificar, p.ex., tipos diferentes de arquivos com um nome de arquivo de início igual, digite, por exemplo, **texto*.***.

Selecione agora a pasta onde os arquivos deverão ser protegidos, clicando no botão avançado. Selecione agora o local de armazenamento onde os arquivos a serem protegidos estão localizados. O Otimizador protegerá agora os arquivos correspondentes definidos apenas nessa pasta (p.ex., status de jogos somente na respectiva pasta de jogo).

Programação

Através da guia **Programação**, é possível definir quando e em que ritmo a tarefa de otimização automática deve ocorrer. Em **Executar**, insira uma predefinição que você pode especificar em **Período**.

Em **Diariamente**, é possível definir com o auxílio dos dados em **Dias da semana** que, p.ex., o seu computador só executará a otimização em dias úteis ou mesmo a cada dois dias ou, nos fins de semana onde ele não é utilizado para trabalhar. Para alterar registros de datas e de períodos em **Período**, selecione com o mouse o elemento que deseja alterar (p.ex., **Dia**, **Hora**, **Mês**, **) e**) e utilize as teclas ou os ícones de setas à direita do campo de entrada, para se movimentar de forma cronológica no respectivo elemento.

Quando não desejar que nenhuma otimização seja realizada, remova simplesmente a marcação da **Verificação do sistema**.

Operação do firewall

Nos capítulos seguintes você recebe informações detalhadas sobre a funcionalidade do firewall G Data. Trata-se aqui de informações específicas que não são utilizadas necessariamente no funcionamento normal do firewall.

Status

Na área de status do Firewall, você obtém informações básicas sobre a situação atual do seu sistema e do Firewall. Essas podem ser encontradas à direita do respectivo registro como informações em texto ou número. Além disso, o status do componente é indicado graficamente. Com um clique duplo no respectivo registro (ou, através da seleção do registro e um clique no botão Edita) você pode tomar providências diretamente aqui ou alternar para a respectiva área do programa.

Assim que tiver otimizado as configurações de um componente com o ícone de aviso, o ícone na área de status torna-se novamente verde.

- **Segurança**: Enquanto você utiliza o computador para o seu trabalho diário, o Firewall aprende cada vez mais que programas você utiliza para o acesso à Internet e que programas são ou não um risco para a segurança. Dependendo do seu nível de conhecimento sobre o assunto tecnologia de firewall, poderá configurar o seu firewall de forma que ele ofereça uma proteção básica muito boa sem fazer perguntas demais, ou uma proteção profissional que se adapte ao seu comportamento de utilização do computador, mas que requeira de sua parte alguns conhecimentos como usuário.

- **Modo**: Aqui você será informado sobre as configurações básicas de acordo com as quais o Firewall está sendo utilizado. As possibilidades aqui são a Criação manual de regras ou o Automático (**Piloto automático**).

  Automático (Piloto automático): Aqui o Firewall trabalha de forma totalmente autônoma e evita os perigos automaticamente de PCs residenciais. Essa configuração oferece uma proteção geral prática e é, na maioria dos casos, recomendável.

Criação manual de regras: Se desejar configurar o seu Firewall de forma individual ou não desejar que determinados aplicativos não trabalhem junto com o Piloto automático, poderá ajustar a sua proteção de Firewall através da criação manual de regras totalmente às suas necessidades pessoais.

- **Rede**: O firewall monitora naturalmente todas as atividades da rede, como uma rede dial-up e uma conexão LAN. Se uma ou mais redes não tiverem que ser protegidas, porque p.ex., foram definidas manualmente como exceção do monitoramento do Firewall, isso é indicado por um ícone de aviso. Um clique duplo no respectivo registro abre uma janela de diálogo, através da qual é possível configurar individualmente regras e definições para a rede selecionada. Em Conjunto de regras, selecione se a respectiva rede deverá fazer parte das redes confiáveis, das redes não confiáveis ou das redes a serem bloqueadas.

A configuração **conexão direta com a Internet** se orienta ao máximo possível nas configurações válidas também para **redes confiáveis**.

A cada **rede** é possível atribuir um **Conjunto de regras** especial. Enquanto você, na área **Redes** visualiza quais redes estão existentes no seu computador, na área **Conjunto de regras**, você vê quais os conjuntos de regras automáticos ou criados por você estão disponíveis no firewall.

- **Ataques registrados**: Assim que o firewall registra um acesso ao seu computador, este será impedido e protocolado aqui. Clicando nos pontos de menu, você receberá mais informações.
- **Radar de aplicativos**: O Radar de aplicativos exibe os programas que estão sendo bloqueados pelo Firewall no momento. Se você desejar permitir que o aplicativo bloqueado acesse a rede, basta selecioná-lo e clicar no botão **Permitir**.

Redes

Na área de redes, são listadas as redes (por ex. LAN, DFÜ, etc.) com as quais o seu computador está conectado. Aqui também será exibido de acordo com qual conjunto de regras (consulte o capítulo **Conjunto de regras**) a respectiva rede será protegida. Se você remover a marcação da respectiva rede, essa será retirada da proteção do firewall. No entanto, você só deve desativar a proteção em casos específicos isolados. Se você marcar a rede com o mouse e clicar no botão Editar, você poderá ver ou alterar as configurações de firewall para essa rede.

Editar rede

Na edição de configurações de rede, existe a opção de utilizar o assistente de regras ou o modo de edição avançado. Geralmente recomenda-se o assistente de regras, porque ele ajudará o usuário na criação de regras e configurações.

- **Informações sobre a rede**: Aqui você obtém informações sobre a rede, como informações do endereço IP, se existente, máscara da subrede, gateway padrão, servidor DNS e WINS.
- **Firewall ativo nessa rede**: Aqui você pode desativar o Firewall para a rede, mas só deverá fazê-lo em casos específicos fundamentados.
- **Utilização compartilhada da conexão à Internet**: Em conexões diretas com a internet, é possível definir se todos os computadores da rede devem ter ou não acesso à internet através de um computador conectado à internet. Essa liberação da conexão à internet (ICS) geralmente pode ser ativada para uma rede doméstica.
- **Permitir configuração automática (DHCP)**: Na conexão do seu computador com a rede, é fornecido um endereço IP dinâmico (através do DHCP = Protocolo dinâmico de configuração de host). Se estiver conectado com a rede através dessa configuração padrão, deverá deixar a marcação.
- **Conjunto de regras**: Aqui você pode escolher rapidamente entre os conjuntos de regras pré-estruturados e definir, dessa forma, se trata-se p. ex., de uma rede confiável, não confiável ou a ser bloqueada em relação aos critérios de monitoramento do Firewall. Com o botão **Editar conjunto de regras** você tem também a possibilidade de configurar individualmente os conjuntos de regras. Para isto, leia também o capítulo **Conjunto de regras**.

Conjunto de regras

Nessa Área é possível criar regras especiais para diferentes redes. Essas regras são então respectivamente reunidas em um conjunto de regras. Conjuntos de regras são predefinidos para a conexão direta com a internet, redes não confiáveis, redes confiáveis e redes a serem bloqueadas. Na visualização geral, é exibido o respectivo conjunto de regras com o nome. Com a ajuda dos botões **Novo**, **Excluir** e **Editar** você pode alterar conjuntos de regras existentes ou adicionar novos.

Os conjuntos de regras predefinidos para a conexão direta com a Internet, redes não confiáveis, redes confiáveis e redes a serem bloqueadas não podem ser excluídos. Conjuntos de regras adicionais criados por você podem naturalmente ser excluídos a qualquer momento.

Criar conjunto de regras

Você pode atribuir a cada rede um **Conjunto de regras** próprio (ou seja, uma coleção especial de regras definidas para isso). Dessa maneira, é possível proteger redes de forma diferente com níveis de risco diferenciados. Assim, uma rede doméstica privada precisa seguramente de menos proteção (e também trabalho de gerenciamento) do que uma de transmissão de dados remotos que está em contato direto com a Internet.

O firewall contém três conjuntos de regras predefinidos para os seguintes tipos de rede:

- **Conjunto de regras para uma rede não confiável**: Aqui estão incluídas em geral as redes abertas, como redes dial-up que têm acesso à Internet.
- **Conjunto de regras para uma rede confiável**: Confiáveis são em geral as redes domésticas e empresariais.
- **Conjunto de regras para uma rede a ser bloqueada**: Quando for necessário bloquear o contato de um computador a uma rede, por um período ou permanentemente, essa configuração pode ser utilizada. Isso faz sentido, por exemplo, na conexão com redes estranhas, sobre as quais não se tem certeza do padrão de segurança (p.ex. em LAN houses, redes empresariais de estranhos, locais de trabalho públicos para notebooks, etc.).

Você pode atribuir um selecionado conjunto de regras correspondente para redes que acabam de ser estabelecidas no seu computador. Além disso, com o botão Novo, é possível criar novos conjuntos de regras para redes. Para isso, clique na área de Conjunto de regras no botão Novo e defina na caixa de diálogo que aparece o seguinte:

- **Nome do conjunto de regras**: Insira aqui um nome significativo para o conjunto de regras.
- **Criar um conjunto de regras vazio**: Aqui você pode criar um conjunto de regras totalmente vazio e preenchê-lo exclusivamente com regras próprias.
- **Criar um conjunto de regras que contenha uma regra útil**: Nessa opção, você pode decidir se no novo conjunto de regras deverão ser definidas regras básicas para redes não confiáveis, confiáveis e redes a serem bloqueadas. Com base nessas predefinições, é possível então efetuar as alterações individuais.

O novo conjunto de regras aparecerá agora na área de conjunto de regras abaixo do respectivo nome (por ex., Novo conjunto de regras) na lista. Se agora, você clicar em **Editar**, dependendo da configuração feita em **Outros** (consulte o capítulo de mesmo nome) aparece o **Assistente de regras** ou a **caixa de diálogo avançado** para a edição das regras individuais desse conjunto de regras. Para saber como atribuir novas regras aos conjuntos de regras, leia os capítulos **Utilizar Assistente de regras** ou **Utilizar o modo de trabalho avançado**.

Além da inserção direta de regras, você tem também, naturalmente, a possibilidade de criar regras através da caixa de informações do Alarme do firewall. Este processo de aprendizado do Firewall é explicado no capítulo **Alarme do Firewall**.

Utilizar o Assistente de regras

Com o Assistente de regras, você pode definir regras adicionais para o respectivo conjunto de regras ou alterar as regras existentes. Principalmente para usuários que não têm bons conhecimentos sobre o assunto Tecnologia de firewall, recomendamos utilizar o Assistente de regras, e não a Caixa de diálogo avançada.

Com o Assistente de regras, você pode alterar uma ou mais regras para o respectivo conjunto de regras selecionado. Ou seja, você cria sempre uma regra dentro de um conjunto de regras, que contém diversas regras.

Dependendo do conjunto de regras definido para a respectiva rede, um aplicativo pode estar bloqueado em um conjunto de regras (p. ex., para redes não confiáveis) e na outra, ter total acesso à rede (p. ex. para redes confiáveis). Dessa forma, você pode, p.ex., restringir um navegador com diferentes regras correspondentes para que ele possa acessar páginas disponíveis em sua rede local, mas que não tenha nenhuma possibilidade de acessar conteúdo na rede de transmissão de dados remotos.

O Assistente de regras disponibiliza as seguintes regras básicas:

- **Permitir ou negar o acesso de um determinado aplicativo**: Através dessa opção é possível selecionar objetivamente um aplicativo (programa) no seu disco rígido e permitir ou proibir explicitamente o acesso à rede, definido através do conjunto de regras. Para isso, selecione no assistente o programa desejado (**Caminho do programa**) e informe em **Direção da conexão** se o programa deve ser bloqueado para conexões de entrada, conexões de saída ou tanto para conexões de entrada como para conexões de saída. Dessa forma, você pode, p.ex., impedir que o software do seu MP3 repasse dados sobre seus hábitos de áudio (conexão de saída) ou cuidar para que atualizações automáticas do produto sejam executadas (conexões de entrada).
- **Abrir ou bloquear um serviço da Internet específico (Porta)**: As **Portas** são áreas de endereço especiais que encaminham dados transmitidos através de uma rede automaticamente a um determinado Protocolo e com isso, a determinados softwares. Dessa forma é feita a transação da transmissão de sites comuns através da porta 80 por exemplo, o envio de e-mails através da porta 25, a captura de e-mails através da porta 10 e assim por diante. Sem o firewall, normalmente todas as portas do seu computador estão abertas, apesar de que a maioria não é necessária a usuários comuns. Através do bloqueio de uma ou mais portas é possível fechar brechas de segurança rapidamente, que podem, caso contrário, ser utilizadas por hackers para ataques. No assistente você tem a possibilidade de bloquear completamente as portas ou apenas para um aplicativo específico (p.ex., o seu software de reprodução de MP3).

- **Permitir ou negar compartilhamento de arquivos e impressora (NetBIOS)**: A **NetBIOS** é uma interface especial em redes e pode ser utilizada para efetuar a liberação de arquivos ou impressão diretamente de computador para computador sem utilizar para isso o protocolo TCP/IP. Como isso, na maioria das redes domésticas, não é necessário, a NetBIOS pode ser usada por hackers para influenciar um computador; é aconselhável em muitos casos negar essa liberação para redes não confiáveis.
- **Permitir ou negar serviços de domínio**: Um **Domínio** é um tipo de diretório estrutural para computadores em uma rede e permite com isso, uma administração centralizada dos computadores vinculados em uma rede. A liberação para serviços de domínio em redes não confiáveis deve ser recusada por via de regra.
- **Permitir utilização compartilhada da conexão à Internet**: Em conexões diretas com a internet, é possível definir se todos os computadores da rede devem ter ou não acesso à internet através de um computador conectado à internet. Essa liberação da conexão à internet (ICS) geralmente pode ser ativada para uma rede doméstica.
- **Alternar para o modo avançado de edição**: Com essa opção, você pode alternar do Assistente de regras para a Caixa de diálogo avançada. Informações sobre a Caixa de diálogo avançada podem ser encontradas no capítulo **Utilizar o modo de trabalho avançado**.

Se remover a marcação em **Iniciar o assistente de regras também no futuro**, o firewall abrirá automaticamente a Caixa de diálogo avançada para as novas regras.

Utilizar o modo de trabalho avançado

No modo de trabalho avançado, você pode definir regras bastante individuais para a respectiva rede, contanto que tenha determinados conhecimentos sobre segurança de rede. Naturalmente, todas as regras podem ser criadas através do Assistente de regras, porém, configurações mais avançadas podem ser efetuadas. Para isso, as seguintes possibilidades estão disponíveis:

- **Nome**: Aqui é possível alterar, se necessário, o nome para o conjunto de regras atual. O conjunto de regras será exibido na lista na área **Conjunto de regras** e poderá ser combinado com as redes identificadas pelo Firewall.

- **Modo furtivo**: Com o modo furtivo: (oculto, escondido) as consultas ao computador, que servem para verificar a acessibilidade das respectivas portas, não são respondidas. Isso dificulta aos hackers a obtenção de informações sobre o sistema.
- **Ação, caso nenhuma regra se aplique**: Aqui é possível definir se o acesso à rede deve ser em geral permitido, recusado ou regulado sob solicitação. Se outras regras forem definidas para programas individuais através da função autodidata do firewall, estas serão naturalmente consideradas.
- **Modo adaptativo**: O modo adaptativo auxilia você com os aplicativos que utilizam a chamada Tecnologia de canal reverso (por ex., FTP e diversos jogos on-line). Esse tipo de aplicativo se conecta a um computador remoto e trata com ele um canal reverso, a partir do qual o computador remoto se "reconecta" com o seu aplicativo. Se o modo adaptativo estiver ativo, o firewall reconhece esse canal reverso e permite o acesso sem consultar especificamente.

Regras

Na lista de regras, você pode encontrar todas as regras definidas como Exceções para esse conjunto de regras. Dessa forma, p.ex., é possível permitir aos programas selecionados Acessos à rede abrangentes, mesmo se a rede não tiver sido definida como confiável. As regras que entram aqui podem ter sido criadas de diferentes formas:

- Através do **Assistentes de regras**
- Diretamente através da **caixa de diálogo avançado**Através do botão Novo
- na caixa de diálogo da caixa Info, que aparece em um Alarme do Firewall.

Naturalmente, cada conjunto de regras tem uma lista própria com regras.

Como as Regras do Firewall são estruturadas parcialmente de forma hierárquica, em alguns casos, é importante observar a classificação das regras. Assim, pode ocorrer que uma liberação de uma porta seja novamente bloqueada através da recusa do acesso a um protocolo. É possível alterar a seqüência da classificação de uma regra marcando-a com o mouse e movendo-a com a seta em **Classificação** para cima ou para baixo na lista.

Se você criar uma nova regra através da caixa de diálogo avançada ou alterar uma regra existente através da caixa de diálogo Editar, aparece a caixa de diálogo **Editar regra** com as seguintes possibilidades de configuração:

- **Nome**: Aqui é encontrado, em regras predefinidas e geradas automaticamente, o nome do programa para o qual a respectiva regra se aplica. O nome pode ser alterado **a qualquer momento ou informações complementares adicionadas através do botão** Editar.
- **Regra ativa**: Uma regra pode ser desativada removendo a marcação sem ter que excluir a regra.
- **Comentário**: Aqui você obtém informações sobre como a regra foi gerada. Em regas predefinidas para o conjunto de regras é exibido **Regra predefinida** e, em regras que foram geradas a partir da caixa de diálogo do **Alarme do Firewall** é exibido **gerado por solicitação** e, para as regras geradas por você mesmo através da caixa de diálogo avançada, você pode inserir o seu próprio comentário.
- **Direção da conexão**: Com a **direção**, é definido se isso refere-se a uma regra para conexões de entrada, de saída ou de entrada e saída para essa regra.
- **Acesso**: Aqui é definido se o acesso deve ser permitido ou negado dentro desse conjunto de regras para o respectivo programa.
- **Registro**: Aqui você pode selecionar que Registros de conexão você deseja permitir ou recusar para um acesso. Aqui você tem a possibilidade de bloquear ou liberar registros em geral, ou acoplar a utilização do protocolo com o uso de um determinado ou de diversos aplicativos (atribuir aplicativos). Da mesma forma, é possível definir exatamente as portas indesejadas ou desejadas através do botão **Atribuir serviço da Internet**.
- **Janela de tempo**: Você pode estruturar o acesso aos recursos da rede de forma dependente de tempo e, p.ex., cuidar para que um acesso só ocorra durante o seu horário de trabalho e não fora desse horário.
- **Espaço de end. IP**: Principalmente para redes com endereços IP fixo atribuídos, faz sentido regulamentar sua utilização através de uma restrição de espaço de endereço IP. Um espaço de endereço IP definido claramente, reduz significativamente o perigo de um ataque de hacker.

Alarme do Firewall

Em geral, o Firewall pergunta no modo **Criação manual de regras** se o acesso de programas e processos desconhecidos que querem se conectar à rede deve ser permitido ou recusado. Para isso, é aberta uma caixa de informações que fornece detalhes sobre o respectivo aplicativo. Aqui você tem a possibilidade de permitir ou recusar uma vez ou permanentemente o acesso à rede para o aplicativo. Assim que você permite ou recusa o acesso permanente a um programa, isso é registrado como **regra** no **conjunto de regras** das respectivas redes, e não será mais perguntado a partir desse momento.

Os seguintes botões estão disponíveis para isso:

- **Permitir sempre**: Com este botão, você cria uma regra para a aplicação mencionada acima (por ex. Opera.exe ou Explorer.exe ou iTunes.exe) que permite um acesso permanente à rede ou à internet na rede da referida aplicação. Você encontra essa regra também como uma regra gerada por consulta na área**Conjunto de regras**
- **Permitir temporariamente**: através desse botão, você permite ao respectivo aplicativo, um acesso único à rede. Na próxima tentativa de um acesso à rede por esse programa, o firewall irá novamente solicitar a permissão.
- **Recusar sempre**: Com este botão, você cria uma regra para a aplicação mencionada acima (por ex. dialer.exe ou spam.exe ou trojan.exe) que nega um acesso permanente à rede ou à internet na rede da referida aplicação. Você encontra essa regra também como uma regra gerada por consulta na área**Conjunto de regras**
- **Bloquear temporariamente**: através desse botão, você recusa uma única vez o acesso à rede do respectivo aplicativo. Na próxima tentativa de um acesso à rede por esse programa, o firewall irá novamente solicitar a permissão.

Outras informações sobre **Protocolo**, **Porta** e **Endereço IP** podem ser obtidas no próprio aplicativo com o qual você deseja interagir.

Registro

Na Área de registros são registradas todas as conexões com a rede e Internet permitidas e bloqueadas pelo Firewall. Essa lista pode ser organizada da forma desejada, clicando nos respectivos títulos das colunas e clicando no botão Detalhes, para obter mais informações sobre cada conexão.

Utilização do backup

A utilização do software é em princípio intuitiva e estruturada de forma clara. Com o auxílio de diferentes guias que podem ser selecionadas por meio dos ícones exibidos à esquerda, você alterna para a respectiva área do programa e lá pode executar ações, informar predefinições ou verificar processos.

Estão disponíveis as seguintes áreas do programa:

- **Status**: na área de status você obtém informações básicas sobre a situação atual das suas medidas de segurança de dados.
- **Salvar**: nessa área, é possível iniciar diretamente os backups ou criar programações para backups automáticos.
- **Restaurar**: aqui é possível restaurar novamente os arquivos de backup armazenados.
- **Ações**: na área de **Ações**, você pode utilizar recursos de FTP e de gravação adicionais.
- **Registros**: todos os processos de backup de dados, administração e de restauração são registrados pelo software G Data e podem ser consultados.

Além disso, você encontra várias funções e possibilidades de configuração na barra de menu superior da interface do programa.

Opções: Aqui você pode alterar as configurações básicas para o funcionamento do software G Data e adaptá-las às necessidades individuais.

Status

Na área **Status**, você recebe uma visão geral sobre todos os status de backup. Aqui você obtém informações sobre quando ocorreu o último Backup e vê quando o próximo Backup automático será iniciado pelo programa.

Salvar

Nessa área do programa é possível iniciar o backup de seus dados mais importantes imediatamente, ou também definir um backup automático que fará o backup de seus dados em intervalos regulares.

Existe a possibilidade de escolher entre as variantes **Backup padrão** e **Backup avançado** entre as quais é possível alternar por meio do respectivo ícone acima, à direita. Aqui é gravado, em primeira linha, o backup padrão. Para o backup avançado, leia o capítulo: **Backup avançado**

Selecione primeiro se você planeja um backup de unidades ou um backup de arquivos:

- **Backup de unidades**: Trata-se de um backup completo de discos rígidos ou partições em uma pasta, que pode ser reproduzido com a função **Restaurar** em caso de perda de dados.
- **Backup de arquivos**: Trata-se de um backup de determinados arquivos e pastas selecionados em uma pasta, que pode ser reproduzido com a função **Restaurar** em caso de perda de dados.

Não há nenhuma opção, nesses arquivos compactados, de procurar por arquivos ou pastas individuais ou gravar de volta novamente. Isso só é possível após a restauração.

Arquivos de origem

Selecione aqui os arquivos que o Backup deve conter. No **Backup de unidades**, você pode marcar as partições de discos rígidos ou outros armazenamentos em massa.

No **Backup de arquivos**, você pode selecionar as pastas predefinidas por padrão do Windows para imagens, música, documentos, filmes e e-mails e, além disso, selecionar também pastas ou tipos de arquivos adicionais para um backup.

- **Imagens**: Se a marcação for colocada aqui, o software G Data armazena todos os tipos de arquivos que contêm imagens e que se encontram em determinadas pastas.
- **Música**: Se esta função for selecionada, o software salva todos os tipos de arquivos que contêm música e que se encontram em determinadas pastas.

- **Documentos**: Também é possível fazer o Backup de formatos diferente de documentos de texto.
- **Filmes**: O software G Data também salva arquivos de filmes de todos os formatos.
- **E-Mail**: O software também possibilita fazer Backups de seus e-mails. Para isso, são armazenadas as **pastas de e-mail dos** programas de e-mail que se encontram no seu computador.
- **Outros tipos de arquivos**: Se utilizar documentos que deseja armazenar no Backup apesar de não terem um formato de arquivo padrão, poderá definir aqui outros tipos de arquivos.

  Portanto, quando desejar fazer o backup de, por exemplo, outros documentos de texto além dos documentos do Office, como documentos no formato OpenOffice, poderá defini-los por meio da guia **Tipos de arquivos** com o botão **Adicionar**. Ou seja, p.ex., insira aqui para documentos do OpenOffice***.odt**. Para excluir formatos de documentos desnecessários do Backup, poderá selecionar o tipo de arquivo desejado e clicar no botão **Remover**.

- **Pastas adicionais de pesquisa**: Em geral, o software G Data cria um backup de pastas e arquivos previstos pelo sistema operacional para o armazenamento de seus dados pessoais. Se tiver pastas em outro local que devam ser consideradas pelo Backup, selecione-as aqui. Essas pastas serão então sempre verificadas quando você desejar o Backup de Imagens, Música, Documentos e etc.
- **Pastas/arquivos adicionais**: Se desejar definir pastas inteiras ou determinados arquivos, independentemente dos tipos de arquivos selecionados para o Backup, poderá fazê-lo aqui. Para isso, basta selecionar as pastas e os arquivos que devem ser considerados pelo software G Data .

  Na área **Seleção de arquivos**, clicando no sinal de mais (+), você pode abrir e selecionar os diretórios, cujo conteúdo será então exibido na visualização de arquivo (à direita). Cada diretório ou arquivo com uma marcação será considerado pelo softwareG Data durante o backup de dados. Se nem todos os arquivos tiverem que ser verificados em um diretório, haverá uma marcação em cinza nesse diretório.

Destino

Aqui é possível definir o destino, ou seja, o local onde o software G Data deverá criar a cópia de segurança dos arquivos e das pastas. O destino selecionado no momento será exibido. Se der um clique duplo nesse registro, é aberta uma caixa de diálogo onde será possível definir um novo destino. Isso pode ser uma unidade de CD ou DVD ROM, um outro Disco rígido, um Pen-drive, outras Mídias removíveis ou um diretório na Rede.

Para salvar backups no G Data **servidor de FTP**, coloque uma marcação na opção **Copiar pasta para o servidor de FTP**.

Se não conseguir obter uma conexão para o **Servidor de FTP**, informe na caixa de diálogo avançada os dados de conexão obtidos no registro do softwareG Data .

Preste atenção para que o backup não seja feito no mesmo disco rígido onde se encontram os dados originais. Se ocorrer um defeito nesse disco, os dados originais e de backup serão perdidos. O mais recomendável é armazenar o backup em um local separado dos arquivos originais, por ex., em uma outra sala em um disco rígido USB, na rede em um servidor de FTP ou gravados em CD/ DVD-ROM.

Programação

Se agora você clicar no botão **Iniciar**, o backup será executado diretamente. Mas você também pode automatizar o backup e solicitar a execução automática ao software G Data em horários específicos regularmente. Para isso, coloque a marcação no respectivo campo para marcação. Informações avançadas sobre a programação podem ser encontradas no capítulo **Programação**.

Restaurar

Na área **Restaurar**, é possível restaurar os seus arquivos originais após uma perda de dados, com base nos seus dados de backup armazenados. Para isso, basta clicar no botão **Restaurar**.

Existe a possibilidade de escolher entre as variantes **Backup padrão** e **Backup avançado** entre as quais é possível alternar por meio do respectivo ícone acima, à direita. Aqui é gravado, em primeira linha, o backup padrão. Para o backup avançado, leia o capítulo: **Backup avançado**

Ações

Nessa área, entre outras coisas, você poderá executar ações para o cuidado e manutenção de seus dados de backup. Os seguintes Programas de serviço estão disponíveis para isso:

Fazer a manutenção das pastas de backup on-line

Se fizer o backup de seus dados mais importantes on-line no **Servidor de FTP da** G Data, naturalmente o software G Data precisará dos respectivos dados de acesso. Aqui é possível inserir o **nome do servidor**, **a porta**, **o nome de usuário**, **a senha** e **o diretório** que foram disponibilizados a você após o registro no servidor de atualização da G Data.

Espaço para backup on-line incluído (1 GB): Com o registro deste software, a G Data disponibiliza gratuitamente 1 GB de espaço para backup on-line em um **servidor de FTP** para os seus backups. Os dados de FTP necessários são assumidos automaticamente na máscara de FTP do seu software G Data e, dessa forma, você poderá manter seus dados seguros on-line e, em caso de necessidade, protegidos por senha. Você receberá os **dados de acesso de FTP** necessários após o registro do software, em um e-mail de confirmação.

Para **Licenças múltiplas** é disponibilizado naturalmente 1 GB de espaço para backup on-line para cada licença, ou seja, para uma licença tripla, três vezes 1 GB.

Enquanto você estiver coberto(a) pelas atualizações de assinaturas de vírus da G Data , esse **espaço para backup por FTP** também estará disponível para você. Em caso de encerramento do contrato, você terá mais 30 dias para remover os seus dados do servidor de backup G Data. Após esse prazo, os dados serão excluídos.

Navegador de FTP

Insira os seus dados de acesso de FTP para obter um acesso ao seu servidor de FTP G Data. Esses dados foram enviados por e-mail após o registro on-line de seu produto. No Navegador de FTP, você pode realizar agora as seguintes ações:

Conectar: Se a conexão para o navegador de FTP for interrompida, ela poderá novamente ser ativada aqui.

Desconectar: Aqui é possível desconectar a conexão para o navegador de FTP.

Nova pasta: Se desejar salvar seus backups em diversas pastas (p.ex., pastas especiais apenas para backups de música), com essa função, será possível criar pastas no seu local de armazenamento de FTP.

Excluir: Com essa função é possível excluir pastas de backup desnecessárias.

Atualizar: Se durante a utilização do navegador de FTP, você tiver executado uma outra **Atualização** poderá solicitar a exibição dos novos dados através do botão **Atualizar**.

Download: Por meio desta função é possível copiar pastas de backup selecionadas com o mouse, do servidor de FTP para um local de armazenamento desejado no seu computador.

Transferir: Através dessa função, é possível posteriormente salvar pastas de backup criadas com o software G Data no seu servidor de FTP.

Gravar depois a pasta de backup em CD/DVD

Arquivos de backup podem também ser gravados posteriormente em um CD ou DVD. Para isso, procure na janela de diálogo que aparece, um projeto que você deseja gravar e clique no botão **Continuar**. Selecione agora a Unidade na qual deseja gravar o backup dos dados.

- **Verificar dados após a gravação**: Se colocar uma marcação nessa opção, os dados gravados serão verificados mais uma vez após a gravação. Isso demora um pouco mais do que um processo de gravação sem verificação, mas é, em geral, recomendável.
- **Copiar arquivos do programa de restauração**: Se ativar essa função, além dos dados de backup arquivados no local de armazenamento do seu backup de dados, será reproduzido um programa, com o qual será possível restaurar os seus dados mesmo sem o software G Data instalado. Para isso, a partir do CD/DVD-ROM inicie o programa **AVKBackup** ou **AVKBackup.exe**.

Clique no botão **Gravar** para iniciar o processo de gravação. Após o processo de gravação, o CD/DVD de backup será automaticamente ejetado.

Naturalmente, os dados de backup não serão excluídos da mídia de dados original. A gravação em CD/DVD posterior é uma segurança adicional.

Através da função **Importar pastas** é possível integrar pastas de backup em mídias de dados externas, como CD ou DVD, novamente no sistema de gerenciamento de dados do software G Data .

Importar pastas

Para restaurar pastas e backups de dados que não estejam em uma unidade administrada pelo software G Data , utilize a função **Importar pastas**. Uma janela de diálogo é aberta, na qual será possível procurar pelos arquivos compactados com a extensão **ARC** desejados, p.ex., em um CD, DVD ou na rede. Se tiver encontrado a pasta de backup desejada, coloque uma marcação e clique, em seguida, no botão **OK**. Uma janela informará que a pasta de backup foi importada com sucesso. Se agora desejar utilizar essa pasta para a restauração de dados, basta ir para a área **Restaurar** do software G Data , selecionar o backup desejado e iniciar a restauração.

Os arquivos comprimidos criados pelo software G Data têm a extensão de arquivo **ARC**.

Criar CD de boot

O BootCD é uma ferramenta útil para tornar computadores já infectados livres de vírus. Principalmente para computadores que, antes da instalação do software G Data não tinham nenhuma proteção antiVirus, recomenda-se a utilização de um BootCD. As informações sobre como criar e utilizar um **CD de boot** podem ser lidas no capítulo: **BootScan antes da instalação**. Com a ajuda do BootCD, também backups podem ser restaurados. Portanto, é recomendável criar um BootCD quando se utiliza a função de backup.

As funções descritas, como por exemplo, a criação de um CD de boot não estão disponibilizadas? Pode ser que a opção **Criar CD de boot** não tenha sido instalada com o software G Data. Esta pode ser facilmente instalada posteriormente, inserindo novamente o CD do software e executando a instalação com a opção BootCD.

Registros

A área Registro cria um **arquivo de registro** abrangente para cada ação e para cada tarefa de backup. Aqui é possível abrir ações individuais com um clique duplo e, se necessário, imprimir ou salvar como arquivo de texto.

Backup avançado

Um Backup avançado é auxiliado pelo assistente e é mais abrangente. Aqui é possível definir diversas tarefas de backup independentes entre si e, dessa forma, executar p.ex, um backup de sua coleção de músicas todos os meses, enquanto que o backup de importantes documentos de texto é feito diariamente. Para iniciar o assistente para criação de uma nova tarefa de backup, clique no botão **Novo**.

Tipo de backup

Selecione primeiro se você planeja um backup de unidades ou um backup de arquivos:

- **Backup de unidades**: Trata-se de um backup completo de discos rígidos ou partições em uma pasta, que pode ser reproduzido com a função **Restaurar** em caso de perda de dados.
- **Backup de arquivos**: Trata-se de um backup de determinados arquivos e pastas selecionados em uma pasta, que pode ser reproduzido com a função **Restaurar** em caso de perda de dados.

Seleção de arquivos

Agora, uma janela é aberta na qual é possível selecionar arquivos e pastas que deseja armazenar. Coloque uma marcação na frente da respectiva pasta ou do arquivo.

Na área **Seleção de arquivos**, clicando no sinal de mais (+), você pode abrir e selecionar os diretórios cujo conteúdo será então exibido na visualização de arquivo (à direita). Cada diretório ou arquivo com uma marcação será considerado pelo software G Data durante o backup de dados. Se nem todos os arquivos tiverem de ser verificados em um diretório, haverá uma marcação em cinza nesse diretório.

Seleção do destino

Aqui é possível definir o destino, ou seja, o local onde o software G Data deverá criar a cópia de segurança dos arquivos e das pastas. Isso pode ser uma unidade de CD ou DVD ROM, um outro Disco rígido, um Pen-drive, outras Mídias removíveis ou um diretório na Rede.

Para salvar backups no servidor de FTP G Data, coloque uma marcação na opção **Copiar pasta para o servidor de FT**.

Se não conseguir obter uma conexão para o **servidor de FTP**, informe na caixa de diálogo avançada os dados de conexão obtidos no **registro** do software G Data .

Preste atenção para que o backup não seja feito no mesmo disco rígido onde se encontram os dados originais. Se ocorrer um defeito nesse disco, os dados originais e de backup serão perdidos. O mais recomendável é armazenar o backup em um local separado dos arquivos originais, por ex., em uma outra sala em um disco rígido USB, na rede em um servidor de FTP ou gravados em CD/ DVD-ROM.

Programação

Em **Executar o backup completo**, informe a frequência, os dias e o horário em que o backup deverá ocorrer. Assim, no turno escolhido, será automaticamente criado um Backup de todos os dados selecionados em **Arquivos de origem**.

Atenção: O Backup automático não funciona com CD-ROM ou DVD-ROM, porque aqui, será necessário a intervenção do usuário na troca da mídia.

Na seção **Excluir pastas antigas**, é possível definir como o software G Data deverá proceder com backups já existentes. O software G Data armazena os seus dados respectivamente em um único arquivo com a extensão **ARC**. Os arquivos de backup que não forem sobregravados, aumentam naturalmente a segurança de seus dados, porque, mesmo no caso do arquivo de backup atual ser danificado, um backup antigo estará disponível, ou seja, nem todos os arquivos serão perdidos. No entanto, as pastas de backup precisam de muito espaço nas mídias de dados e você deverá prestar atenção em não juntar arquivos de backup em excesso. O recomendável é informar em **Manter os backups completos** uma quantidade máxima de backups que serão armazenados na sua mídia de backup. A respectiva pasta de backup mais antiga será então substituída pela mais recente.

> **Atenção**: Para poder executar backups programados, é necessário colocar uma marcação na área **Opções** em **Dados do usuário**, no registro **Executar tarefa como** e lá, informar os dados de acesso para a sua **Conta do usuário do Windows**. Essas informações são necessárias para que o backup também possa ser executado de forma programada quando você não estiver registrado como usuário.

Backups parciais

Os Backups parciais servem para fazer um backup mais rápido dos dados. Ao invés de utilizar todos os dados para um backup, o backup parcial estrutura-se em um backup completo existente e salva apenas os dados que tiverem sido alterados desde o último backup completo ou foram recentemente criados. Dessa forma, um Backup completo do seus dados está á disposição onde o processo de backup é executado muito mais rapidamente. Se desejar utilizar um Backup parcial, coloque a marcação em **Criar backup(s) parcial(is)** e defina em que turno o Backup deverá ser feito.

> A desvantagem do Backup parcial é um comparável aumento da necessidade de espaço de armazenamento, porque os dados não mais necessários no Backup completo não são excluídos diretamente. Após o próximo Backup completo, os dados do Backup completo e do parcial serão novamente reunidos e a quantidade de dados será a mesma que em um Backup completo.

Diferencial / Incremental: No backup diferencial, todos os dados, que foram alterados desde o último backup completo ou adicionados recentemente são armazenados. Serão sempre anexados no último backup completo. Em comparação com um novo backup completo, economizam-se tempo e espaço de armazenamento. O backup incremental vai ainda uma etapa adiante e salva, entre dois backups parciais, os arquivos que foram alterados de backup parcial a backup parcial. A desvantagem aqui é que, em uma restauração dos dados, são necessárias várias pastas.

Opções

Na área Opções você pode alterar as opções gerais para pastas compactadas. Em geral, não é necessário efetuar aqui nenhuma alteração porque as opções padrão G Data abrangem a maioria das aplicações.

Opções gerais de pastas

Nas opções gerais de pastas de backup, existem as seguintes possibilidades de configuração:

- **Limitar o tamanho do arquivo da pasta**: Se você gravar as **Pastas** em CD/DVD-ROM ou outras mídias graváveis, é importante que o software G Data limite o tamanho desses arquivos compactados. Aqui, você tem uma opção de tamanhos padrão que permitem o armazenamento posterior dos dados de backup em CD, DVD ou discos Blu-ray. A pasta de backup será divida no tamanho máximo informado e as informações de backup serão distribuídas em uma ou mais pastas de backup.
- **Excluir pastas temporárias**: Essa opção deve em geral permanecer ativada. As pastas de backup temporárias exigem muito espaço no disco rígido após uma determinada quantidade de processos de backup, e não serão mais necessárias após a sua utilização temporária.
- **Copiar arquivos do programa de restauração**: Se ativar essa função, além dos dados de backup arquivados no local de armazenamento do seu backup de dados, será reproduzido um programa, com o qual será possível restaurar os seus dados mesmo sem o software G Data instalado. Para isso, a partir do CD/DVD-ROM inicie o programa **AVKBackup** ou **AVKBackup.exe**.

O programa de restauração será agora copiado em CD/DVD-ROM. No caso de cópias de segurança em mídias removíveis (pen-drives e discos rígidos externos), isso não será feito.

Se tiver instalado o softwareG Data no computador no qual a restauração deverá ser feita, não execute a restauração com o programa de restauração no CD/DVD-ROM, mas através da função **Pastas compactadas importar**.

- **Verificar vírus antes do arquivamento**: Quando o módulo AntiVirus estiver instalado, será possível verificar a existência de vírus nos seus dados, antes que esses sejam armazenados na pasta de backup.
- **Verificar pasta após a criação**: Essa função serve para verificar a pasta de backup após sua criação, mais uma vez quanto à integralidade e perfeição.
- **Criptografar a pasta de backup**: Se desejar proteger seus arquivos em pasta contra o Acesso de estranhos, poderá atribuir uma **senha**. A restauração dos dados, só poderá então ser feita com essa senha. Você deverá decorar essa senha ou anotar em local seguro. Sem a senha, os seus dados de arquivos não poderão mais ser restaurados.
- **Teste de integridade no backup diferencial**: Essa função serve para verificar um **backup parcial** após sua criação, mais uma vez quanto à integralidade e perfeição.
- **Teste de integridade na restauração do disco rígido**: Após uma restauração, essa função serve para verificar a regravação dos dados novamente.

- **Diretório para arquivos temporários**: Os **arquivos temporários** são dados que o softwareG Data grava no seu disco rígido apenas temporariamente. Se não houver espaço suficiente na sua partição padrão, é possível alterar aqui a partição e o local de armazenamento temporário para esses arquivos.

Dados do usuário

Para poder executar backups programados, é necessário colocar uma marcação na área **Opções** em **Dados do usuário**, no registro **Executar tarefa como** e, informar os **Dados de acesso** para a sua **Conta do usuário do Windows**. Essas informações são necessárias para que o backup também possa ser executado de forma programada quando você não estiver registrado como usuário.

Compressão

Na área **Compressão** é possível definir o nível de compactação de seus arquivos ou pastas.

- **Boa compressão**: Os dados serão fortemente compactados para o Backup. Com isso você economiza espaço de armazenamento do backup, mas esse demorará mais tempo.
- **Compressão equilibrada**: A compressão do Backup não será tão forte, mas esse será executado mais rápido.
- **Execução rápida**: Nenhuma compressão é feita, mas o Backup será executado mais rapidamente.

Ignorar arquivos

Em geral, o software G Data salva arquivos com base no seu formato de arquivo. No seu sistema de computador encontram-se formatos de arquivo correspondentes também em áreas que são administradas automaticamente e não relevantes para o backup, porque os respectivos arquivos só foram armazenados temporariamente (p.ex., para aceleração da exibição de páginas da Internet). Para que o softwareG Data não armazene esses arquivos desnecessariamente, é possível ignorá-los colocando a respectiva marcação.

- **Diretório temporário com arquivos**: Quando essa opção tiver sido selecionada, as **pastas temporárias**, assim como as subpastas e os arquivos lá existentes, não são incluídas no backup de dados.
- **Diretório temporário da Internet com arquivos**: Quando essa opção tiver sido selecionada, as pastas para a gravação de páginas da internet, assim como as subpastas e os arquivos lá existentes, não são incluídas no backup de dados.
- **Thumbs.db**: quando essa opção tiver sido selecionada, os arquivos **thumbs.db** criados automaticamente pelo Windows Explorer, não são incluídos no backup de dados. Esses arquivos servem para administrar a exibição em miniatura de slideshows e são criados automaticamente a partir das imagens originais.
- **Arquivos temporários (atributo de arquivo)**: quando essa opção tiver sido selecionada, os arquivos com o atributo de arquivo **temporário** atribuído pelo sistema, não são incluídos no backup.
- **Arquivos de sistema (atributo de arquivo)**: quando essa opção tiver sido selecionada, os arquivos com o atributo de arquivo **Arquivo de sistema** atribuído pelo sistema, não são incluídos no backup.

Com a função **Ignorar tipos de arquivos**, é possível definir as extensões de arquivo que não devem ser consideradas no seu backup. Para isso, proceda da seguinte forma: Em **Tipo de arquivo** (por ex., ***.txt**), informe a extensão ou o nome do arquivo que deseja ignorar. Clique agora em **OK**. Repita o procedimento para todos os outros tipos e nomes de arquivos que deseja ignorar, por ex., **picasa.ini**, ***.ini**, ***bak**, etc. O símbolo do asterisco e o ponto de interrogação podem ser utilizados aqui como curinga.

A forma de funcionamento dos **Espaços reservados** é a seguinte:

O **ponto de interrogação** (?) é substituto para caracteres individuais.

* O **asterisco** (*) é substituto para seqüências de caracteres inteiras.

Para verificar todos os arquivos com a extensão de arquivo **exe**, digite ***.exe**. Para verificar p.ex., formatos de planilhas diferentes (p. ex.,***.xlr**, ***.xls**), basta digitar ***.xl?**. Para verificar tipos diferentes de arquivos com um nome de arquivo de início igual, digite, por exemplo, **text*.***.

Redefinir opções padrão atuais

O clique neste botão assume as opções para o software G Dataque foram definidas como padrão. Portanto, se tiver definido inadvertidamente as opções falsas na criação do backup e não souber como corrigi-las, clique no botão **Redefinir para as opções padrão**.

Utilizar Windows Shadow Copy

Se esta opção for desativada, não se pode criar uma imagem da partição do sistema durante a operação em andamento.

Restaurar

Se tiver salvado os seus dados com a função **Backup avançado**, na área **Restaurar**, você terá também opções avançadas. Portanto, aqui, será possível acessar novamente Pastas importadas e selecionar a versão do backup que deseja utilizar. Quando tiver selecionado um Backup de dados e clicar no botão e **Restaurar**, será perguntado se deseja restaurar todos os arquivos (**Restaurar todos os arquivos da pasta compactada**) ou apenas arquivos selecionados (**Restaurar somente os arquivos selecionados da pasta compactada**). Faça aqui a sua escolha.

Seleção do destino

Na caixa de diálogo a seguir, é possível definir se os dados deverão ser exatamente restaurados no local onde ocorreu o backup ou, se deseja salvar os arquivos em uma pasta especial. Em geral, recomenda-se a configuração **Restaurar os arquivos no diretório original**. Em **Senha**, digite a senha de acesso se tiver compactado o seu backup protegido por senha. Em **Sobregravar arquivos existentes**, é possível definir como o software G Data deverá proceder com arquivos que, ao reproduzir o backup de dados, ainda existam no local de origem. Para isso, as seguintes possibilidades estão disponíveis:

- **sobregravar sempre**: Nessa configuração, os arquivos do backup de dados serão sempre vistos como mais importantes do que os dados que se encontram no diretório original. Se uma marcação for colocada aqui, os dados existentes ainda serão totalmente sobregravados pelos dados que estão na pasta de backup.
- **quando o tamanho tiver sido alterado**: com essa configuração, os dados existentes no diretório original só serão sobregravados se o arquivo original tiver sido alterado. Arquivos não alterados em relação ao tamanho serão ignorados. Dessa forma, a restauração de dados poderá possivelmente ser mais rápida.
- **quando o período 'Alterado em' na pasta de backup for mais recente**: com essa opção, os arquivos no diretório original serão sempre substituídos pelas cópias na pasta de backup quando forem mais recentes. Aqui também uma restauração dos dados poderá ser mais rápida porque, possivelmente, nem todos os arquivos terão de ser restaurados, mas apenas os dados alterados.
- **quando o período 'Alterado em' tiver sido alterado**: aqui, os dados no diretório de origem serão sempre substituídos quando a data de alteração em comparação com os arquivos compactados do backup tiver sido alterada.

Em seguida, clique em **Concluir**. Os seus dados serão em seguida restaurados para o local definido.

Manuseio da Proteção infantil

Com a proteção infantil é possível controlar o comportamento na navegação e a utilização do computador para suas crianças. Em princípio, o manuseio da Proteção infantil é autoexplicativo e projetado de forma clara. Com o auxílio de diferentes guias que podem ser selecionadas por meio dos ícones exibidos à esquerda, você alterna para a respectiva área do programa e lá pode executar ações, informar predefinições ou verificar processos.

A Proteção infantil não é instalada com a instalação padrão do software G Data. No entanto, isso poderá ser feito a qualquer momento através de uma instalação personalizada (consulte o capítulo **Instalação**).

Além disso, você encontra várias funções e possibilidades de configuração na barra de menu superior da interface do programa.

Testar: Aqui, como administrador, você pode verificar se as restrições para determinados usuários têm o efeito desejado. No **modo de teste**, você pode selecionar páginas com o seu navegador da web que deveriam estar bloqueadas e confirmar se as configurações estão corretas.

Configurações: aqui você pode alterar as configurações básicas para o funcionamento da Proteção infantil e adaptá-las às necessidades individuais.

Status

Na área de Status, você, como administrador, pode selecionar em **Usuário**, o usuário para o qual deseja fazer alterações e configurações, além disso, é possível também criar novos usuários.

Os usuários que já tenham um **perfil de usuário do Windows** no seu computador, podem ser selecionados diretamente em **Usuário**. Para alterar configurações aqui, selecione o usuário desejado e clique no botão Editar.

Criar novo usuário

Clique no botão **Novo usuário**. Uma caixa de diálogo é aberta onde você pode inserir o nome de usuário e a senha para esse usuário.

Do aspecto da segurança, uma **Senha** deverá ter pelo menos oito caracteres, conter letras maiúsculas e minúsculas, assim como números.

Em seguida, em **Usuário**, aparecerá o novo nome de usuário criado e, ao mesmo tempo, será criada uma **conta de usuário do Windows** para esse usuário. Isso significa que a proteção infantil estará automaticamente ativa para a pessoa que se conectar com o seu nome de usuário na inicialização do Windows, com as respectivas configurações. Dê agora um clique duplo com o mouse na área de configurações que devem ser definidas para esse usuário, ou seja, a interdição de **Conteúdo proibido** ou a liberação exclusiva de **Conteúdo permitido** ou defina para esse usuário, se o **Monitorar tempo de utilização da Internet (atividade de fato na Internet)** ou **Monitorar tempo de utilização do computador** deverá ser monitorado.

Conteúdo proibido

Nessa área é aberta uma janela de diálogo na qual você pode permitir conteúdos especiais na Internet para o usuário exibido no momento. Para isso, selecione as categorias desejadas que devem ser bloqueadas inserindo uma marcação. Clique agora em OK e as páginas da Internet que correspondem aos **Critérios de bloqueios** serão bloqueadas.

> Se clicar no botão Novo, será aberta uma janela de diálogo onde é possível definir seus próprios **Critérios de bloqueio** (também chamadas de **Blacklists**). Para isso, defina primeiro os nomes e, se necessário, um texto informativo para o filtro criado individualmente.

Se clicar agora em OK, uma nova janela será aberta onde é possível reunir os conteúdos que devem ser suprimidos por esse filtro. Digite em **Filtro**, um termo que deva ser bloqueado e, em **Local para a pesquisa**, a área de um site onde deva ocorrer a pesquisa.

Você tem as seguintes opções:

- **URL**: Se colocar a marcação aqui, o texto a ser bloqueado será procurado no **endereço da web**. Se desejar interditar páginas como www.chatcity.no, www.crazychat.co.uk ou semelhante, basta colocar chat como filtro, a marcação em **URL** e clicar no botão **Adicionar**. Serão bloqueadas todas as páginas que utilizarem de alguma forma o **Nome do domínio**, ou seja, no **endereço da Internet** a seqüência de letras chat.
- **Título**: Se colocar a marcação aqui, o texto a ser bloqueado será procurado no título do site da web. Esta é a área que você vê, p.ex., quando quer **marcar** uma página da sua **lista de favoritos** como um **marcador de livro**. Se desejar interditar páginas como Chat City Detroit, Teenage Chat 2005 ou semelhante, basta colocar chat como filtro, a marcação em **Título** e clicar no botão **Adicionar**. Serão bloqueadas todas as páginas que utilizarem de alguma forma no título, a seqüência de letras chat.
- **Meta**: As chamadas **Metatags** são registros de texto ocultos em sites, que servem para listá-las em **mecanismos de busca** de forma mais útil ou apenas com mais freqüência. Termos de pesquisa como sexo ou chat são bastante utilizados para aumentar os acessos à página. Se desejar interditar páginas que tenham chat em algum lugar da metatag, basta colocar chat como filtro, a marcação em **Meta** e clicar no botão **Adicionar**. Serão bloqueadas todas as páginas que utilizarem de alguma forma nas metatags a seqüência de letras chat.
- **No texto completo**: Se desejar verificar o conteúdo legível de uma página diretamente em relação ao conteúdo a ser bloqueado - p.ex., ***chat*** - coloque a marcação no texto completo e clique em seguida no botão **Adicionar**. Serão bloqueadas todas as páginas que contenham de alguma forma no texto da página exibida a seqüência de letras ***chat***.

Naturalmente pode ocorrer que **termos de filtragem** muito genéricos bloqueiem páginas que são inofensivas. Assim, um termo como pica faria também que registros como Picasso fossem bloqueados.

Páginas especiais que caiam na classificação do filtro por engano podem ser novamente liberadas explicitamente, através da função **Exceção**. Para isso, basta clicar no botão **Exceção** e inserir no filtro a palavra Picasso como exceção.

Filtros criados por você podem ser editados ou excluídos como desejados na área **Meus filtros**. Para isto, leia o caítulo **Próprio filtro**.

Conteúdo permitido

Através dessa área é aberta uma janela de diálogo na qual você pode permitir conteúdos especiais na Internet para o usuário exibido no momento. Para isso, selecione as categorias desejadas que devem ser permitidas inserindo uma marcação. Clique agora em OK e as páginas da Internet que correspondem aos critérios desejados serão permitidas.

Se clicar no botão Novo, é aberta uma janela de diálogo onde é possível definir o conteúdo próprio a ser permitido (também chamadas de **Whitelists**). Para isso, defina primeiro os nomes e, se necessário, um texto informativo para o filtro criado individualmente.

Clique agora em **OK**. É aberta uma caixa de diálogo onde você pode preencher a Whitelist com páginas da web que p.ex., são adequadas a crianças. Insira em **Filtro**, que **parte do nome do domínio** deve ser permitido. Se por exemplo, você desejar liberar um site com conteúdo adequado às crianças, poderá inserir aqui www.elefante.dee permitir com isso, o acesso a esse site. Insira agora em **Descrição**, o que pode ser encontrado nesse site, p.ex., Elefante - site adequado às crianças e, em **Link para o serviço**, insira o endereço exato do site. A Descrição e o link para o serviço são importantes quando o seu filho realmente abrir uma página não permitida. Ao invés de uma mensagem de erro, aparece uma página HTML no navegador, que lista todos os sites inseridos na Whitelist, incluindo as descrições. Dessa forma, o seu filho poderá acessar novamente as páginas que são permitidas. Quando todas as informações tiverem sido inseridas, clique em **Adicionar**, e a Whitelist será complementada com essas informações.

O **Filtro** procura segmentos nos nomes dos domínios. Dependendo das informações no filtro, os resultados podem ser diferentes. Pode ser útil fazer diferentes restrições de acordo com cada site.

Monitorar tempo de utilização da Internet

Aqui você pode determinar por quanto tempo e quando o usuário selecionado terá acesso à internet. Para isso, coloque a marcação em **Monitorar tempo de utilização da Internet**. Agora, você pode definir quanto tempo o usuário pode usar a Internet no total por mês, quanto tempo por semana e quantas horas em determinados dias da semana. Dessa forma, os fins de semana podem ter tratamentos diferentes dos dias da semana para crianças em idade escolar. Os respectivos períodos podem ser inseridos para isso em **Dias/hh:mm**, onde, por exemplo, uma entrada **04/20:05** daria um tempo de utilização de 4 dias, 20 horas e 5 minutos na Internet.

Em relação aos dados para a utilização da Internet, contam sempre respectivamente, os valores menores. Se você determinar um limite temporário de quatro dias em um mês, mas permitir, por exemplo, cinco dias para a semana, o software limitará a utilização da internet automaticamente para quatro dias.

Quando o respectivo usuário tentar acessar a Internet acima do contingente de tempo, aparece uma tela de informações no navegador, que informa que seu contingente foi ultrapassado.

Bloquear períodos

Através do botão **Bloquear períodos**, você pode abrir um campo de diálogo onde poderá bloquear categoricamente períodos especiais na semana, adicionalmente à restrição total da utilização da Internet. Períodos bloqueados são representados em vermelho e os liberados em verde. Para liberar ou bloquear um período, basta marcá-lo com o mouse. Em seguida, aparecerá ao lado do cursor do mouse, um menu contextual onde você terá duas possibilidades: **Liberar período** e **Bloquear período**. Quando o respectivo usuário tentar acessar a Internet durante os períodos bloqueados, aparece uma tela de informações no navegador, que o informa que nesse período, ele não tem direito ao acesso à Internet.

Monitorar tempo de utilização do computador

Aqui é possível definir quanto tempo e em que períodos os usuários selecionados podem acessar a Internet. Para isso, coloque a marcação em **Monitorar tempo de utilização do computador**. Agora, você pode definir quanto tempo o usuário pode utilizar o computador no total por mês, quanto tempo por semana e quantas horas em determinados dias da semana. Dessa forma, os fins de semana podem ter tratamentos diferentes dos dias da semana para crianças em idade escolar. Os respectivos períodos podem ser inseridos para isso em **Dias/hh:mm**, onde, por exemplo, uma entrada **04/20:05** daria um tempo de utilização de 4 dias, 20 horas e 5 minutos na Internet. Através do botão **Exibir aviso antes da expiração do tempo**, é possível informar ao usuário um pouco antes do computador ser desligado automaticamente, para que esse possa salvar seus dados. Se o computador for desligado sem um aviso, isso poderá levar a Perdas de dados.

Em relação aos dados para a utilização do computador, contam sempre, respectivamente, os valores menores. Então, se você definir para o mês uma restrição de tempo de quatro dias, mas permitir na semana cinco dias, o software reduz a utilização do usuário automaticamente para quatro dias de uso do computador.

Próprio filtro

Nesta área, você pode modificar as suas listas de whitelists (conteúdos permitidos) e blacklists (conteúdos proibidos) propriamente criadas e criar listas completamente novas manualmente.

Os seguintes tipos de lista são basicamente diferenciados entre si:

- **Whitelist**: Se você selecionar uma Whitelist para um dos usuários selecionados acima, ele só poderá ver as páginas da web que se encontrem nessa Whitelist. Na área **Dados básicos**, você pode estruturar, como administrador, essa Whitelist de acordo com o desejado ou selecionar uma lista adequada para um usuário nas Whitelists predefinidas. Uma whitelist é especialmente adequada para permitir um acesso bem restrito à Internet para crianças pequenas e, também dar a possibilidade de utilizar sites com conteúdo pedagógico recomendado, mas nada além disso.

- **Blacklist**: Com uma Blacklist você pode bloquear sites selecionados para um usuário. Fora isto, o usuário terá livre acesso à Internet. Observe que através desta função, você poderá bloquear sites especiais, mas que um conteúdo semelhante poderá estar disponível também em outros sites da web. Uma Blacklist de endereços da Internet nunca é, nesse sentido, uma proteção completa contra conteúdo indesejado.

Uma Whitelist não pode ser utilizada ao mesmo tempo que uma Blacklist, já que a Whitelist por si, já possibilita as maiores restrições de acesso possíveis.

Os botões a seguir possibilitam a você a edição das Listas de exclusão:

- Excluir: O recurso **Excluir** permite excluir de forma simples com o mouse as listas selecionadas.
- Novo: Através desse recurso você pode criar uma Blacklist ou Whitelist totalmente nova. O procedimento para isso, é o mesmo descrito no capítulo Conteúdo proibido e Conteúdo permitido .
- Editar: Com isso você pode alterar o conteúdo de uma lista existente.

Registros

Na área de registros, você, como administrador, tem uma visão geral sobre todas as tentativas de abertura de conteúdo proibido por outros usuários. Acima, você pode além disso, selecionar o usuário na lista cujo registro você deseja solicitar a exibição.

Esses registros também podem ser naturalmente excluídos no botão **Excluir registros**.

Configurações: Nesta área, você pode modificar configurações essenciais para as informações na área de registro. Dessa forma, é possível definir se as infrações contra conteúdo permitido e/ou proibido devem ser registradas ou não. Quando o conteúdo é registrado, você pode visualizar os registros dos diversos usuários na área de registro.

Como os Arquivos de registro podem ficar muito grandes com a utilização constante, você pode, a partir da Proteção infantil em **Exibir mensagem quando o arquivo atingir___KB**, solicitar o lembrete informando que o arquivo de registro ultrapassou um determinado tamanho e, na Área de registro em **Excluir registros**, exclui-lo manualmente.

Saiba mais

Aqui você pode obter informações sobre funções importantes do programa do software.

BootScan

O **BootScan** ajuda a combater vírus que se aninharam em seu computador antes da instalação do software antivírus e que, possivelmente, podem impedir a instalação do G Data software. Para isso, existe uma versão especial do programa do Software que pode ser executada já antes da inicialização do Windows.

O que significa um processo de inicialização? Quando você liga o seu computador, normalmente, o sistema operacional Windows é iniciado automaticamente. Este processo se chama **Dar um boot**. Existe também a possibilidade de iniciar outros programas automaticamente, ao invés do sistema operacional Windows. Para verificar a existência de vírus no seu computador antes da inicialização do Windows, a G Data disponibiliza, adicionalmente à versão do Windows, uma versão especial com capacidade de boot.

Como eu cancelo um BootScan? Se, após uma reinicialização, o seu computador não mostrar o habitual ambiente do Windows, mas uma interface especial do software G Data, isso não deverá ser motivo para preocupações. Se não tiver planejado nenhum BootScan, basta selecionar com as teclas de seta o registro **Microsoft Windows** e clicar em **Voltar**. O Windows inicializará normalmente, sem o BootScan.

Se desejar executar um **BootScan**, proceda da seguinte forma:

1a **BootScan com o CD do programa**: Utilize o CD do programa da G Data e faça com ele o boot no seu computador. - Insira o CD da G Data na unidade. Na janela de inicialização aberta, clique em **Cancelar** e desligue o seu computador.

1b **Faça o BootScan com o software G Data descarregado da Internet**: Através do registro Criar CD de boot da **G Data** no grupo de programas da **G Data** (*ícone do Windows na barra de tarefas > Todos os programas > Software G Data > Criar CD de boot*), você grava um novo BootCD.

Insira o seu próprio BootCD gravado na unidade. Na janela de inicialização aberta, clique em **Cancelar** e desligue o seu computador.

Se você usa o **Windows XP**, pode acontecer que, na tentativa de criar um BootCD, receba uma mensagem que o **IMAPI 2.x** não está instalado. Trata-se de uma atualização do Microsoft para sistemas operacionais antigos que é necessária para gravar mídias de dados. Você pode descarregar a atualização necessária diretamente da página inicial da Microsoft e instalá-la.

1c **Você tem uma versão especial para netbook do software G Data em um pen drive?** Aqui é possível executar o BootScan diretamente através do pen drive. No entanto, para isto, o seu netbook terá que ser capaz de dar o boot a partir de um pen drive.

Conecte o **G Data pen drive** com o seu netbook. Na janela de inicialização aberta, clique em **Cancelar** e desligue o Netbook.

Após a primeira etapa o BootScan para as três variações tem o mesmo procedimento:

2 Reinicialize o computador. O menu de inicialização do G Data **BootScan** aparece.

3 Com as setas, selecione a opção G Data**BootCD** e confirme a seleção com **Enter**. Um sistema operacional Linux será iniciado pelo CD e aparecerá uma versão especial da G Data para BootScans.

Se tiver problemas com a visualização da interface do programa, reinicialize o seu computador e selecione a opção G Data **BootCD – Alternativo**.

4 O programa irá sugerir agora a atualização das assinaturas de vírus.

Se você utiliza uma versão do software G Data que é compatível com as funções de backup, aqui você tem a possibilidade adicional de iniciar diretamente a reprodução de backups de seus dados armazenados.

5 Clique agora em **Sim**. Para poder executar a atualização, você deve inserir seus dados de acesso já recebidos ou seu número de registro. Depois disso, você pode executar a atualização. Assim que os dados tiverem sido atualizados na Internet, aparecerá o aviso **Atualização concluída**. Saia agora da tela de atualização clicando no botão **Fechar**.

A **atualização automática na Internet** é disponibilizada quando for utilizado um **roteador** que atribua endereços IP automaticamente (**DHCP**). Se não for possível a atualização na Internet, o **BootScan** poderá ser executado também com as assinaturas de vírus antigas. No entanto, nesse caso, após a instalação do software G Data , você deverá executar o mais rápido possível um novo BootScan com dados atualizados.

6 Agora você verá a interface do programa. Clique no registro **Verificar computador** e o seu computador será agora verificado quanto à existência de vírus e softwares maliciosos. Este processo pode levar uma hora ou mais, dependendo do tipo de computador e tamanho do disco rígido.

7 Se o software G Data encontrar vírus, remova-os com a ajuda da opção sugerida no programa. Após a remoção bem-sucedida do vírus, o arquivo original ficará novamente disponível.

8 Após concluir a verificação de vírus, saia do sistema clicando no x (no canto superior direito da janela).

9 Remova o CD do software G Data da unidade assim que a sua unidade for aberta ou desconecte o pen drive G Data do seu netbook.

10 Desligue novamente o seu computador e o reinicie. Agora, o seu computador inicializará novamente com o sistema operacional Windows padrão e você terá a garantia de poder instalar o software normal da G Data em um sistema sem vírus.

O que faço quando meu computador não faz o boot a partir do CD-ROM?

Se não for possível o boot a partir do CD/DVD-ROM, pode ser que essa opção precise primeiro ser ativada. Isto é feito na chamada **BIOS**, um sistema, que é inicializado automaticamente antes do sistema operacional Windows. Para fazer alterações na BIOS, execute as seguintes etapas:

1. Desligue o seu computador.
2. Reinicialize o computador. Normalmente, você consegue acesso à configuração da BIOS, ao iniciar (= Boot) o computador você pressionar a tecla **Del** (algumas vezes também a tecla **F2** ou **F10**).
3. A forma de alteração individual na configuração da BIOS é diferente de computador para computador. Leia para isto, a documentação do seu computador. Em resumo, a sequência do boot deve ser **CD/DVD-ROM:, C:** ou seja, a unidade de CD/DVD-ROM será o **1st Boot Device** e a partição do disco rígido, com o seu sistema operacional Windows, será o **2nd Boot Device**.
4. Salve as alterações e reinicie o seu computador. Agora o computador estará pronto para um BootScan.

O que faço quando o meu netbook (ou também PC desktop/ notebook) não faz o boot a partir do pen drive?

Se o seu computador não fizer o boot automaticamente a partir do pen drive, execute as seguintes etapas:

1. Desligue o seu computador.
2. Insira o G Data **pen drive** em uma **porta USB** livre do seu computador.
3. Ligue o seu computador.
4. Durante a inicialização, pressione a tecla **F2**, para chegar na **BIOS** do computador.
5. A interface da BIOS será exibida com uma barra de menu, onde você pode selecionar o menu **Boot** com as teclas de seta (para direita/esquerda). Agora, pressione **Enter**.
6. Você terá, então, a possibilidade de selecionar o registro **Hard disc drives** através das teclas de seta (para cima/baixo). Agora, pressione **Enter**.
7. Selecione agora o registro **USB** de forma que **1st Drive = USB** apareça em primeiro lugar (teclas **Enter** e de setas).

8. Pressione **F10**, para salvar e fechar a BIOS. O seu computador poderá agora fazer o boot a partir do pen drive.
9. Reinicialize o computador. Agora o computador estará pronto para um BootScan.

Ícone G Data

O software G Data protege o seu computador permanentemente contra vírus e softwares maliciosos. Para que você possa ver que a proteção está ativa, um ícone é exibido na barra de tarefas ao lado do relógio.

Este ícone G Data indica que está tudo em ordem e que a proteção do seu computador está ativa.

Caso a sentinela tenha sido desativada ou existam outros problemas, o ícone G Data exibirá um sinal de aviso. Nesse caso, você deverá iniciar o software G Data o mais rápido possível e verificar as configurações.

Quando o softwareG Data executa um download de dados da Internet, ele também indica isso através de um ícone especial.

Se clicar no ícone com o botão direito do mouse, aparece um menu contextual com o qual se pode controlar os aspectos de segurança fundamentais do software.

As seguintes funções estão disponíveis:

- **G Data** : Com essa opção, ativa-se a **SecurityCenter** e é possível efetuar as configurações para a sentinela de vírus. As possibilidades existentes na SecurityCenter podem ser consultadas no capítulo: **SecurityCenter**
- **Desativar sentinela**: Com esta opção, é possível desativar a **Sentinela de vírus**, em caso de necessidade, e também ativá-la novamente. Isso pode ser útil, p.ex, quando uma grande quantidade de dados em seu disco rígido é copiada de um local para outro ou para rodar processos de exibição que ocupam muito espaço na memória (copiar DVDs e outros). A sentinela de vírus só deve ser desativada quando for realmente necessário e, deve-se ter a certeza de que o sistema durante esse período, se possível, não esteja conectado à Internet ou possa acessar dados novos e não verificados (p.ex, através de CDs, DVDs, placas de memória ou dispositivos USB).

- **Desativar firewall**: Se você usar uma versão do software G Data com firewall integrado, também é possível desativar o **firewall** através do menu contextual, caso necessário. O seu computador estará ainda conectado à Internet e a outras redes, mas não estará protegido contra ataques ou espionagem.
- **Desativar piloto automático**: O **Piloto automático** é uma parte do **Firewall** e decide de forma independente que solicitações e contatos o seu computador deve aceitar ou não através da rede ou Internet. O piloto automático é ideal para uma utilização normal e deverá ser deixado sempre ativado. Como o firewall, o piloto automático está disponível nas versões selecionadas do software G Data.
- **Atualização de vírus**: Um software antivírus deve estar sempre atualizado. Naturalmente, você pode solicitar que atualização dos dados seja executada automaticamente pelo software. No entanto, se você precisar urgentemente de uma atualização, poderá iniciá-la através do botão **Atualização de vírus**. Para saber a utilidade de uma atualização de vírus, pode ser lido no capítulo: **Atualizações**
- **Estatística**: Essa opção permite exibir uma estatística sobre os eventos de verificação.

Verificação de vírus

Com a verificação de vírus, você verifica se o seu computador foi infectado por softwares maliciosos. Quando você inicia a verificação de vírus, esse controla cada arquivo no seu computador, quanto a possibilidade desse poder infectar outros arquivos ou se o próprio já está infectado. Se vírus ou outros softwares maliciosos forem encontrados em uma verificação de vírus, existem diversas possibilidades como o vírus pode ser removido ou tornado inofensivo.

1 Inicie a verificação de vírus. Leia o procedimento para isso no capítulo: **Proteção AntiVirus**

2 Será iniciada uma verificação de seu computador quanto a infecção por vírus. Além disto, é aberta uma janela onde você obtém informações sobre o status da verificação.

Uma barra de progresso na parte superior da janela, indica o progresso da verificação no seu sistema. Já durante a verificação de vírus você terá diversas possibilidades para influenciar o andamento da verificação de vírus:

- **Em caso de sobrecarga suspender a verificação de vírus**: Através desse campo de opções, você pode definir que o software espere com a verificação de vírus, até que as outras atividades no computador tenham sido concluídas.
- **Desligar computador após a verificação de vírus**: Esta função é bastante prática, quando você desejar deixar a verificação de vírus rodando durante a noite ou após o expediente. Assim que a verificação de vírus do software G Data for finalizada, o seu computador será desligado.
- **Pastas protegidas por senha**: Enquanto uma pasta compactada for protegida por senha, o softwareG Data não pode verificar os arquivos desta pasta. Se colocar uma marcação aqui, o software antivírus o informa quais pastas compactadas protegidas por senha não pôde verificar. Contanto que essa pasta não seja descompactada, um vírus ali contido não representa nenhum risco para o seu sistema.
- **Acesso negado**: Em geral, existem arquivos no Windows utilizados exclusivamente pelos aplicativos e que por isso, não podem ser verificados enquanto esses aplicativos estiverem sendo executados. Portanto, o melhor é que nenhum outro programa esteja sendo executado em seu sistema durante uma verificação de vírus. Ao colocar aqui uma marcação, os dados não verificados serão exibidos.

3a Assim que o seu sistema estiver livre de vírus, você poderá, após o término da verificação, sair da janela do assistente, através do botão **Fechar**.

O seu sistema terá sido verificado e estará livre de vírus.

3b Para o caso de vírus e outros programas maliciosos terem sido encontrados, você terá a possibilidade, agora, de decidir como deseja proceder com as detecções de vírus. Normalmente, basta clicar no botão **Executar ações**.

O softwareG Data utiliza então uma configuração padrão (*desde que você não tenha configurado isso diferentemente nas configurações em **AntiVirus > Verificação manual de vírus para arquivos e pastas infectadas***) e desinfecta os arquivos afetados, ou seja, ele os repara de forma que possam ser novamente utilizados sem restrições e não sejam mais perigosos para o seu computador.

Se uma desinfecção não for possível, o arquivo será colocado em quarentena, ou seja, ele será codificado e movido para uma pasta extremamente segura, onde não poderá mais causar danos.

Se esse arquivo infectado ainda for necessário, ele poderá, em casos excepcionais, ser novamente retirado da área da quarentena e utilizado.

O seu sistema terá sido verificado e estará livre de vírus.

3c Quando os arquivos/objetos infectados forem conhecidos e você puder diferenciar quais deles talvez não sejam mais necessários, existe a possibilidade de reagir de forma bastante individual à cada detecção de vírus.

Na listagem das detecções de vírus, é possível, na coluna **Ação**, definir, para cada arquivo infectado, o que deverá ocorrer com o mesmo.

- **Somente registrar**: Na visualização **Registros** a infecção é relacionada. No entanto, não é feita a reparação ou exclusão do arquivo afetado. **Atenção: Quando um vírus for somente registrado ele permanece ativo e perigoso.**
- **Desinfectar (se não for possível: somente registrar)**: Aqui, tenta-se remover o vírus de um arquivo infectado. Se isso não for possível sem danificar o arquivo, o vírus será registrado e você poderá cuidar disso mais tarde, através do registro. **Atenção: Quando um vírus for somente registrado ele permanece ativo e perigoso.**
- **Desinfectar (se não for possível: para quarentena)**: Esta é a configuração padrão. Aqui, tenta-se remover o vírus de um arquivo infectado, se não for possível sem danificar o arquivo, esse é movido para a **Quarentena**. Para isso, leia também o capítulo **Como funciona a quarentena?**
- **Desinfectar (se não for possível: Excluir arquivo**: Aqui tenta-se remover o vírus de um arquivo afetado. Se isso não for possível, o arquivo será excluído. Esta função só deve ser utilizada quando nenhum dado importante existir no seu computador. Uma exclusão de arquivos infectados pode, na pior das hipóteses fazer com que o seu Windows não mais funcione e que uma reinstalação seja necessária.

- **Mover arquivo para a quarentena**: Os arquivos infectados são movidos diretamente para a **Quarentena**. Na quarentena, os arquivos são armazenados criptografados. Ou seja, o vírus não pode causar nenhum dano e o arquivo infectado continuará existente para eventuais tentativas de reparação. Leia para isso também o capítulo: **Como funciona a quarentena?**
- **Excluir arquivo**: Esta função só deve ser utilizada quando nenhum dado importante existir no seu computador. Uma exclusão de arquivos infectados pode, na pior das hipóteses fazer com que o seu Windows não mais funcione e que uma reinstalação seja necessária.

Clicando agora no botão **Executar ações** o softwareG Data procederá da forma definida com cada detecção de vírus.

O seu sistema terá sido verificado quanto à existência de vírus. No entanto, se você tiver utilizado uma configuração com a opção Registrar, é possível que o seu computador não esteja livre de vírus.

4 Ao fim da verificação de vírus, você terá a possibilidade de transmitir uma cópia dos arquivos infectados para nós, para que possamos melhorar a proteção antiVirus para todos os usuários com base nesses dados. Naturalmente os seus dados serão tratados sigilosamente e nenhuma informação pessoal será repassada ou utilizada.

O repasse desses dados é totalmente voluntário e, se desejar, poderá ignorar esse ponto ou desativá-lo de forma permanente.

Vírus detectado

Quando o software G Data encontrar um vírus ou um outro programa malicioso no seu computador, você tem as seguintes possibilidades de tratar o arquivo infectado.

- **Somente registrar**: Na visualização **Registros** a infecção é relacionada. No entanto, não é feita a reparação ou exclusão do arquivo afetado. Porém, através do registro de vírus detectados você pode verificar individualmente os vírus e os remover objetivamente. **Atenção: Quando um vírus for somente registrado ele permanece ativo e perigoso.**

- **Desinfectar (se não for possível: mover para a quarentena)**: Aqui, tenta-se remover o vírus de um arquivo infectado, se não for possível sem danificar o arquivo, esse é movido para a **Quarentena**. Leia para isso também o capítulo: **Como funciona a quarentena?**
- **Mover arquivo para a quarentena**: Os arquivos infectados são movidos diretamente para a **Quarentena**. Na quarentena, os arquivos são armazenados criptografados. Ou seja, o vírus não pode causar nenhum dano e o arquivo infectado continuará existente para eventuais tentativas de reparação. Leia para isso também o capítulo: **Como funciona a quarentena?**
- **Excluir arquivo infectado**: Esta função só deve ser utilizada quando nenhum dado importante existir no seu computador. Uma exclusão de arquivos infectados pode, na pior das hipóteses fazer com que o seu Windows não mais funcione e que uma reinstalação seja necessária.

Quarentena e caixas postais de e-mail: Existem arquivos os quais não é recomendável enviar para a quarentena, p.ex., os arquivos compactados para as caixas postais de e-mail. Quando uma caixa postal de e-mail é enviada para a quarentena, o seu programa de e-mail não poderá mais acessá-la e possivelmente não funcionará mais. Você deve ter cuidado especialmente nos arquivos com a extensão **PST**, pois estes, em geral, contêm os dados de sua **caixa postal de e-mail do Outlook**.

Feedback sobre malwares

Os G Data Security Labs pesquisam constantemente procedimentos para G Data proteger os clientes contra malware. Quanto mais informações existirem, mais eficazes poderão ser os mecanismos de proteção desenvolvidos. No entanto, muitas informações estão contidas em sistemas já atacados ou infectados. Para poder incluir também esse tipo de informação na análise, fundou-se a Iniciativa de informações sobre malware G Data. Nesse âmbito, as informações relevantes a malware são enviadas aos Security Labs G Data. Com a sua participação você contribui para que todos os clientes G Data possam usar a internet com mais segurança.

Malware: É um termo genérico para todos os arquivos, programas e códigos que são programados para infectar, espionar ou controlar um computador sem o conhecimento do usuário. Entre eles estão, por exemplo, vírus, vermes, vírus de rootkit, cavalos de troia, registradores de teclado e muito mais.

Que dados são coletados?

Em princípio, dois tipos de dados são transmitidos: 1. Você pode enviar voluntariamente arquivos de malware para G Data e 2. são detectados conteúdos prejudiciais em uma página da web. Quando você envia arquivos com malware para a Internet Ambulance, além do arquivo, são enviados o local da detecção, o nome original do arquivo e a data da criação. Na detecção de conteúdos maliciosos da Internet, são enviados os seguintes dados:

- Número da versão do produto G Data e do mecanismo utilizado,
- Idioma (local) do sistema operacional,
- URL cujo acesso foi bloqueado e a razão (malware, phishing etc.)
- Nome do malware

Essas informações não são adequadas para identificar usuários do PC. Elas não serão comparadas aos dados pessoais.

Como os dados levantados são utilizados?

No processamento e no armazenamento dos dados, consideram-se os requisitos da lei sobre a proteção de dados e a disponibilização de dados dos respectivos países. G Data trabalha com o maior cuidado para proteger os dados contra acesso não autorizado. A avaliação dos dados acontece nos G Data Security Labs e serve para o esclarecimento de questões de pesquisa na área da segurança TI. A meta mais importante é a pesquisa de riscos de segurança e o desenvolvimento de mecanismos de proteção. Aos exemplos de utilização, pertencem, por exemplo, a criação de listas de bloqueio, a avaliação estatística para publicação em artigos especializados ou o desenvolvimento de conjuntos de regras para a tecnologia de proteção. A participação é voluntária e a recusa não tem nenhum efeito negativo no funcionamento do produto. Com a sua participação na Iniciativa de informações sobre malware G Data, futuramente todos os clientes G Data poderão ser informados e protegidos ainda melhor sobre ameaças de computadores.

Mensagem not-a-virus (não vírus)

Arquivos informados como **not-a-virus**, são aplicativos potencialmente perigosos. Tais programas, não dispõem diretamente de funções maliciosas, mas, no entanto, podem ser utilizados para ataques contra você. Estão incluídos nessa categoria, por exemplo, programas de serviço para administração remota, programas para comutação automática das teclas de função, clientes IRC, servidor de FTP ou programas distintos de serviço para criação ou para ocultar processos.

Quarentena

Durante a verificação de vírus você tem a possibilidade de proceder de diferentes maneiras com as **Detecções de vírus**. Uma opção é mover o arquivo infectado para a quarentena. A quarentena é uma área protegida dentro dentro do software onde os arquivos infectados são armazenados de forma codificada e, dessa forma, o vírus não pode mais ser repassado a outros arquivos.

Os arquivos em quarentena permanecem então no estado em que foram encontrados pelo softwareG Data e você pode decidir como deseja proceder.

- **Atualizar**: Se a caixa de diálogo para a quarentena tiver sido mantida aberta por um longo tempo e um vírus for encontrado e movido para a quarentena, nesse meio tempo, (por exemplo, automaticamente através da sentinela de vírus), a exibição poderá ser atualizada com esse botão.
- **Enviar**: Em determinados casos, você pode enviar um arquivo infectado que não pôde ser desinfectado para a G Data pela Internet. Naturalmente o conteúdo desse arquivo será tratado confidencialmente. O resultado dessa verificação flui para a melhoria e atualização das assinaturas de vírus e do software. Leia para isso também o capítulo: **Feedback sobre malwares**
- **Desinfectar**: Em muitos casos os arquivos infectados podem ainda ser salvos. O software remove então a parte virótica de um arquivo infectado e reconstrói assim, o arquivo original não infectado. Quando uma desinfecção é bem-sucedida, o arquivo é movido automaticamente para o local onde estava armazenado antes da verificação de vírus, e estará novamente disponível sem restrições.

- **Mover de volta**: Às vezes pode ser necessário mover de volta um arquivo infectado que não pôde ser desinfectado da quarentena para seu local de origem. Isso pode ser feito para salvar os dados. Essa função só deve ser utilizada em casos raros e sob rígidas condições de segurança (por ex., desconectar o computador da rede/Internet, fazer o backup antes de dados não infectados etc.).
- **Excluir**: Quando não precisar mais do arquivo infectado, você pode simplesmente exclui-lo da quarentena.

Registros

Na área de registros são listados os registros criados pelo software. Ao clicar no título das colunas **Hora de início**, **Tipo**, **Título** ou **Status**, você pode organizar respectivamente os registros existentes. Com os botões **Salvar como** e **Imprimir** dados de registro podem ser salvos como arquivos de texto ou serem impressos diretamente. Para excluir um registro, selecione o registro na tabela com o mouse e clique na tecla **Del** ou pressione o botão **Excluir**.

Licença múlti-usuário

Com uma licença multiusuário, você pode utilizar o software G Data na quantidade licenciada de computadores. Após a instalação no primeiro computador e da Atualização na Internet, você obterá os Dados de acesso transmitidos on-line. Quando você instalar seu software no próximo computador, você deve simplesmente informar o nome do usuário e a senha que você recebeu no registro no G Dataservidor de atualização. Repita o procedimento em cada instalação.

Utilize em todos os seus PCS os seus **Dados de acesso** (Nome de usuário e Senha) para a atualização na Internet, os quais foram fornecidos após o seu registro. Para isso, proceda como descrito a seguir:

1. Inicie o software G Data.
2. Na SecurityCenter, clique em **Assinaturas de vírus > Atualizar assinaturas de vírus**
3. Insira na janela exibida, os dados de acesso recebidos anteriormente por e-mail . Se clicar agora em OK o seu computador será licenciado.

Prorrogação da licença

Alguns dias antes de sua licença expirar, aparece uma janela de informações na barra de tarefas. Clicando, abre-se uma caixa de diálogo na qual você pode prorrogar a sua licença sem problemas diretamente, em poucos passos. Clique simplesmente no botão **Comprar agora**, complete os seus dados e a proteção antiVirus está novamente garantida imediatamente. A fatura será enviada nos próximos dias pelo correio.

Esta caixa de diálogo aparece apenas ao término de um ano. Depois disso, a sua licença G Data é prorrogada automaticamente a cada ano. Mas você pode cancelar essa assinatura a qualquer hora e sem mencionar as razões.

Troca de computador

Você pode utilizar o seu produto G Data em um novo ou em outro computador com os seus dados de acesso existentes. Instale simplesmente o software e informe os seus dados de acesso. Nesse caso, o servidor de atualização configura a conexão para o novo computador. Caso o software G Data ainda se encontre no antigo computador, é preciso transferir a licença deste para o novo. A quantidade de transferências de licenças é limitada - alcançado o valor limite, a licença é bloqueada completamente e não é mais possível carregar nenhuma atualização.

Desinstalação

Quando desejar remover em algum momento o software G Data do seu computador, a forma mais fácil de fazê-lo é, no G Data**Grupo de programas** , clicar no botão **Desinstalar**. A desinstalação ocorrerá de forma totalmente automática. Como alternativa, é possível executar a desinstalação no painel de controle do Windows.

- **Windows Vista**, **Windows 7**: Na barra de tarefas do Windows, clique no ícone Iniciar (normalmente na parte inferior à esquerda da sua tela) e selecione a pasta **Painel de controle**. Lá você encontrará o item **Programas > Desinstalar programas**. Selecione aqui o software G Data na lista e clique no botão **Desinstalar** para executar a desinstalação.

- **Windows XP**: Clique na barra de tarefas do Windows em **Iniciar** e selecione a pasta **Configurações > Painel de controle > Software**. Lá você encontrará, na guia **Instalar/Desinstalar**, a possibilidade de selecionar o software G Data com o mouse. Clique em seguida no botão **Adicionar/Remover** para executar a desinstalação.

Se durante a desinstalação ainda houverem arquivos na **Quarentena**do software G Data, será perguntado se esses arquivos deverão ser excluídos ou não. Se não excluir os arquivos, eles permanecerão em uma pasta G Dataespecial codificada em seu computador e, dessa forma, não poderão causar danos. Esses arquivos estarão novamente disponíveis quando o software G Data for reinstalado no seu computador. Durante a desinstalação será perguntado se você deseja excluir as **configurações e registros**. Se não excluir esses arquivos, os registros e as configurações estarão novamente disponíveis em uma reinstalação. Conclua a desinstalação clicando no botão Concluir. O software terá sido totalmente desinstalado do seu sistema.

Praga de computador

O **BootScan** ajuda a combater vírus que se aninharam em seu computador antes da instalação do software antivírus e que, possivelmente, podem impedir a instalação do G Data software. Para isso, existe uma versão especial do programa do software que pode ser executada já antes da inicialização do Windows.

O que significa um processo de inicialização? Quando você liga o seu computador, normalmente, o sistema operacional Windows é iniciado automaticamente. Este processo se chama **Dar um boot**. Existe também a possibilidade de iniciar outros programas automaticamente, ao invés do sistema operacional Windows. Para verificar a existência de vírus no seu computador antes da inicialização do Windows, a G Data disponibiliza, adicionalmente à versão do Windows, uma versão especial com capacidade de boot.

Como eu cancelo um BootScan? Se, após uma reinicialização, o seu computador não mostrar o habitual ambiente do Windows, mas uma interface especial do software G Data, isso não deverá ser motivo para preocupações. Se não tiver planejado nenhum BootScan, basta selecionar com as teclas de seta o registro **Microsoft Windows** e clicar em **Voltar**. O Windows inicializará normalmente, sem o BootScan.

Se desejar executar um **BootScan**, proceda da seguinte forma:

1a **BootScan com o CD do programa**: Utilize o CD do programa da G Data e faça com ele o boot no seu computador. - Insira o CD da G Data na unidade. Na janela de inicialização aberta, clique em **Cancelar** e desligue o seu computador.

1b **Faça o BootScan com o software G Data descarregado da Internet**: Através do registro Criar CD de boot da **G Data** no grupo de programas da **G Data** (*ícone do Windows na barra de tarefas > Todos os programas > Software G Data > Criar CD de boot*), você grava um novo BootCD.

Insira o seu próprio BootCD gravado na unidade. Na janela de inicialização aberta, clique em **Cancelar** e desligue o seu computador.

Se você usa o **Windows XP**, pode acontecer que, na tentativa de criar um BootCD, receba uma mensagem que o **IMAPI 2.x** não está instalado. Trata-se de uma atualização do Microsoft para sistemas operacionais antigos que é necessária para gravar mídias de dados. Você pode descarregar a atualização necessária diretamente da página inicial da Microsoft e instalá-la.

1c **Você tem uma versão especial para netbook do software G Data em um pen drive?** Aqui é possível executar o BootScan diretamente através do pen drive. No entanto, para isto, o seu netbook terá que ser capaz de dar o boot a partir de um pen drive.

Conecte o **G Data pen drive** com o seu netbook. Na janela de inicialização aberta, clique em **Cancelar** e desligue o Netbook.

Após a primeira etapa o BootScan para as três variações tem o mesmo procedimento:

2 Reinicialize o computador. O menu de inicialização do G Data **BootScan** aparece.

3 Com as setas, selecione a opção G Data**BootCD** e confirme a seleção com **Enter**. Um sistema operacional Linux será iniciado pelo CD e aparecerá uma versão especial da G Data para BootScans.

Se tiver problemas com a visualização da interface do programa, reinicialize o seu computador e selecione a opção G Data **BootCD – Alternativo**.

4 O programa irá sugerir agora a atualização das assinaturas de vírus.

Se você utiliza uma versão do software G Data que é compatível com as funções de backup, aqui você tem a possibilidade adicional de iniciar diretamente a reprodução de backups de seus dados armazenados.

5 Clique agora em **Sim**. Para poder executar a atualização, você deve inserir seus dados de acesso já recebidos ou seu número de registro. Depois disso, você pode executar a atualização. Assim que os dados tiverem sido atualizados na Internet, aparecerá o aviso **Atualização concluída**. Saia agora da tela de atualização clicando no botão **Fechar**.

A **atualização automática na Internet** é disponibilizada quando for utilizado um **roteador** que atribua endereços IP automaticamente (**DHCP**). Se não for possível a atualização na Internet, o **BootScan** poderá ser executado também com as assinaturas de vírus antigas. No entanto, nesse caso, após a instalação do software G Data , você deverá executar o mais rápido possível um novo BootScan com dados atualizados.

6 Agora você verá a interface do programa. Clique no registro **Verificar computador** e o seu computador será agora verificado quanto à existência de vírus e softwares maliciosos. Este processo pode levar uma hora ou mais, dependendo do tipo de computador e tamanho do disco rígido.

7 Se o software G Data encontrar vírus, remova-os com a ajuda da opção sugerida no programa. Após a remoção bem-sucedida do vírus, o arquivo original ficará novamente disponível.

8 Após concluir a verificação de vírus, saia do sistema clicando no x (no canto superior direito da janela).

9 Remova o CD do software G Data da unidade assim que a sua unidade for aberta ou desconecte o pen drive G Data do seu netbook.

10 Desligue novamente o seu computador e o reinicie. Agora, o seu computador inicializará novamente com o sistema operacional Windows padrão e você terá a garantia de poder instalar o software normal da G Data em um sistema sem vírus.

O que faço quando meu computador não faz o boot a partir do CD-ROM?

Se não for possível o boot a partir do CD/DVD-ROM, pode ser que essa opção precise primeiro ser ativada. Isto é feito na chamada **BIOS**, um sistema, que é inicializado automaticamente antes do sistema operacional Windows. Para fazer alterações na BIOS, execute as seguintes etapas:

1. Desligue o seu computador.
2. Reinicialize o computador. Normalmente, você consegue acesso à configuração da BIOS, ao iniciar (= Boot) o computador você pressionar a tecla **Del** (algumas vezes também a tecla **F2** ou **F10**).
3. A forma de alteração individual na configuração da BIOS é diferente de computador para computador. Leia para isto, a documentação do seu computador. Em resumo, a sequência do boot deve ser **CD/DVD-ROM:, C:** ou seja, a unidade de CD/DVD-ROM será o **1st Boot Device** e a partição do disco rígido, com o seu sistema operacional Windows, será o **2nd Boot Device**.
4. Salve as alterações e reinicie o seu computador. Agora o computador estará pronto para um BootScan.

O que faço quando o meu netbook (ou também PC desktop/ notebook) não faz o boot a partir do pen drive?

Se o seu computador não fizer o boot automaticamente a partir do pen drive, execute as seguintes etapas:

1. Desligue o seu computador.
2. Insira o G Data **pen drive** em uma **porta USB** livre do seu computador.
3. Ligue o seu computador.
4. Durante a inicialização, pressione a tecla **F2**, para chegar na **BIOS** do computador.
5. A interface da BIOS será exibida com uma barra de menu, onde você pode selecionar o menu **Boot** com as teclas de seta (para direita/esquerda). Agora, pressione **Enter**.
6. Você terá, então, a possibilidade de selecionar o registro **Hard disc drives** através das teclas de seta (para cima/baixo). Agora, pressione **Enter**.
7. Selecione agora o registro **USB** de forma que **1st Drive = USB** apareça em primeiro lugar (teclas **Enter** e de setas).

8. Pressione **F10**, para salvar e fechar a BIOS. O seu computador poderá agora fazer o boot a partir do pen drive.
9. Reinicialize o computador. Agora o computador estará pronto para um BootScan.

Dicas de comportamento

Apesar de o software G Data não detectar e remover apenas vírus conhecidos, mas, com a ajuda da análise heurística, reconhecer programas maliciosos desconhecidos até hoje, é sem dúvida melhor evitar logo de vez uma infecção por vírus. Para isso, algumas medidas de segurança devem ser atendidas, que não exigem muito esforço e que, no entanto, aumentam a segurança do seu sistema e dados consideravelmente.

- **Utilizar contas do usuário**: No seu computador você deve utilizar duas contas de usuário. Uma **conta de administrador**, que você sempre utiliza quando instalar softwares ou configurações básicas no seu computador e uma **conta de usuário** com direitos restritos. A conta de usuário, não deverá p.ex., poder instalar programas ou realizar modificações no sistema operacional do Windows. Com essa conta, você poderá então navegar relativamente seguro na Internet, pegar dados de computadores de terceiros e etc. A documentação da ajuda do sistema operacional Windows explica como criar diferentes contas de usuário.
- **Ignorar e-mails spam**: Cartas corrente e e-mails spam não devem ser respondidos por via de regra. Mesmo que esses e-mails não contenham vírus, eles sobrecarregam significativamente o fluxo de dados na Internet através de seu encaminhamento indesejado.
- **Verificar suspeita de vírus**: Se tiver uma suspeita de vírus fundamentada, p.ex., porque um novo software instalado não faz o que era esperado ou uma mensagem de erro aparecer, verifique o respectivo programa preferencialmente antes da reinicialização do computador, quanto à infecção de vírus. Isso é recomendável porque alguns cavalos de tróia executam os comandos de exclusão somente após a reinicialização do computador e, dessa forma, podem ser mais facilmente detectados e combatidos.
- **Windows Updates regulares**: Deve se tornar rotina a instalação dos atuais patches da Microsoft, porque esses fecham freqüentemente novas falhas de segurança detectadas do Windows, antes que um programador de vírus pense em utilizá-las para novas rotinas maliciosas. O Windows-Update também pode ser automatizado.

- **Utilizar software original**: Mesmo quando em raros casos a mídia de dados do software original esteja contaminada por vírus, a probabilidade de uma infecção por vírus através de cópias pirata ou cópias em mídias de dados regraváveis é significativamente maior. Por esse motivo, utilize apenas software original.
- **Tratar software da Internet com cuidado**: Ao fazer download de softwares da Internet, seja extremamente crítico e utilize apenas softwares realmente necessários cuja origem lhe pareça confiável. Nunca abra arquivos enviados por e-mail por desconhecidos ou que chegam de forma supreendente de amigos, colegas ou conhecidos. Verifique antes, através de uma consulta ao local correspondente, se o respectivo aplicativo pode ser iniciado sem perigo ou não.

Índice

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P